

HP 5500 EI & 5500 SI Switch Series Configuration Examples

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.



Part number: 5998-5153

Contents

802.1X configuration examples	1
AAA configuration examples	31
ACL configuration examples	53
ARP attack protection configuration examples	81
ARP configuration examples	92
Proxy ARP configuration examples	95
BPDU tunneling configuration examples	101
CFD configuration examples	107
DHCP configuration examples	116
DLDAP configuration examples	129
DNS configuration examples	138
Ethernet OAM configuration examples	155
HABP configuration examples	158
IGMP configuration examples	161
IGMP snooping configuration example	177
IP addressing configuration examples	193
IP performance optimization configuration examples	196
IP source guard configuration examples	202
IPv6 basics configuration examples	209
IPv6 multicast VLAN configuration examples	213
IPv6 PIM configuration examples	224
Link aggregation configuration examples	258
LLDP configuration examples	273
Login management configuration examples	280
MAC address table configuration examples	288
MAC authentication configuration examples	295
MCE configuration examples	312
Mirroring configuration examples	333
MLD configuration examples	365
MLD snooping configuration examples	381
Multicast VLAN configuration examples	397
NQA configuration examples	408

NTP configuration examples	435
OSPF configuration examples	449
Patch installation examples	493
PIM configuration examples	497
Port isolation configuration examples	529
Port security configuration examples	536
QinQ configuration examples	552
Traffic policing configuration examples	589
GTS and rate limiting configuration examples	613
Priority and queue scheduling configuration examples	618
User profile configuration examples	632
Control plane protection configuration examples	637
QoS policy-based routing configuration examples	645
RRPP configuration examples	657
sFlow configuration examples	722
Smart Link and CFD collaboration configuration examples	727
Smart Link configuration examples	747
Monitor Link configuration examples	767
Software upgrade configuration examples	772
Spanning tree configuration examples	783
SSH configuration examples	810
Static multicast route configuration examples	836
Static routing configuration examples	846
Tunnel configuration examples	861
URPF configuration examples	875
VLAN configuration examples	878
VLAN mapping configuration examples	910
IPv4-based VRRP configuration examples	928
IPv6-based VRRP configuration examples	976

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 5500 EI	Release 2220
HP 5500 SI	

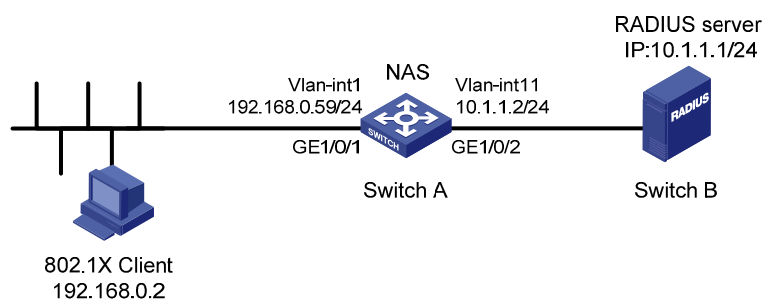
Network requirements

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 HP 5500 HI switch functions as the RADIUS server.

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

Figure 1 Network diagram



Configuration restrictions and guidelines

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

- The authentication port (UDP) used by RADIUS servers is 1812 according to standard RADIUS protocols. However, the port (UDP) is set to 1645 on an HP device that functions as the RADIUS authentication server. You must specify the authentication port as **1645** in the RADIUS scheme on the access device.

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

Configuration procedures

Configuring IP addresses

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

Configuring Switch A

1. Configure the RADIUS scheme:

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

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

New Radius scheme

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 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 GigabitEthernet 1/0/1.

```
[SwitchA] interface gigabitethernet 1/0/1
```

```
[SwitchA-GigabitEthernet1/0/1] dot1x
```

802.1x is enabled on port GigabitEthernet1/0/1.

```
[SwitchA-GigabitEthernet1/0/1] quit
# Configure GigabitEthernet 1/0/1 to implement MAC-based access control. By default, the port
implements MAC-based access control.
[SwitchA] dot1x port-method macbased interface gigabitethernet 1/0/1
# Enable 802.1X globally.
[SwitchA] dot1x
802.1x is enabled globally.
```

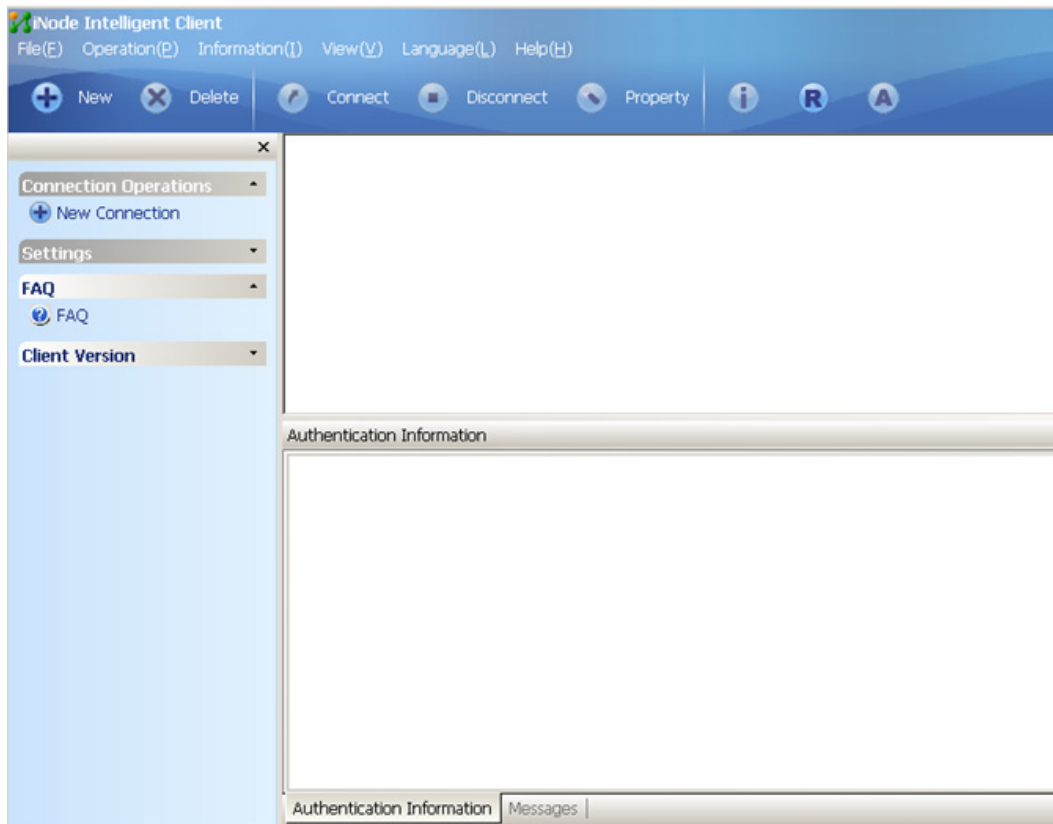
Configuring the RADIUS server

```
# Create RADIUS user guest and enter RADIUS server user view.
<Sysname> system-view
[Sysname] radius-server user guest
# Set the password to 123456 in plain text for RADIUS user guest.
[Sysname-rdsuser-guest] password simple 123456
[Sysname-rdsuser-guest] quit
# Specify RADIUS client 10.1.1.2, and set the shared key to abc in plain text.
[Sysname] radius-server client-ip 10.1.1.2 key simple abc
```

Configuring the 802.1X client

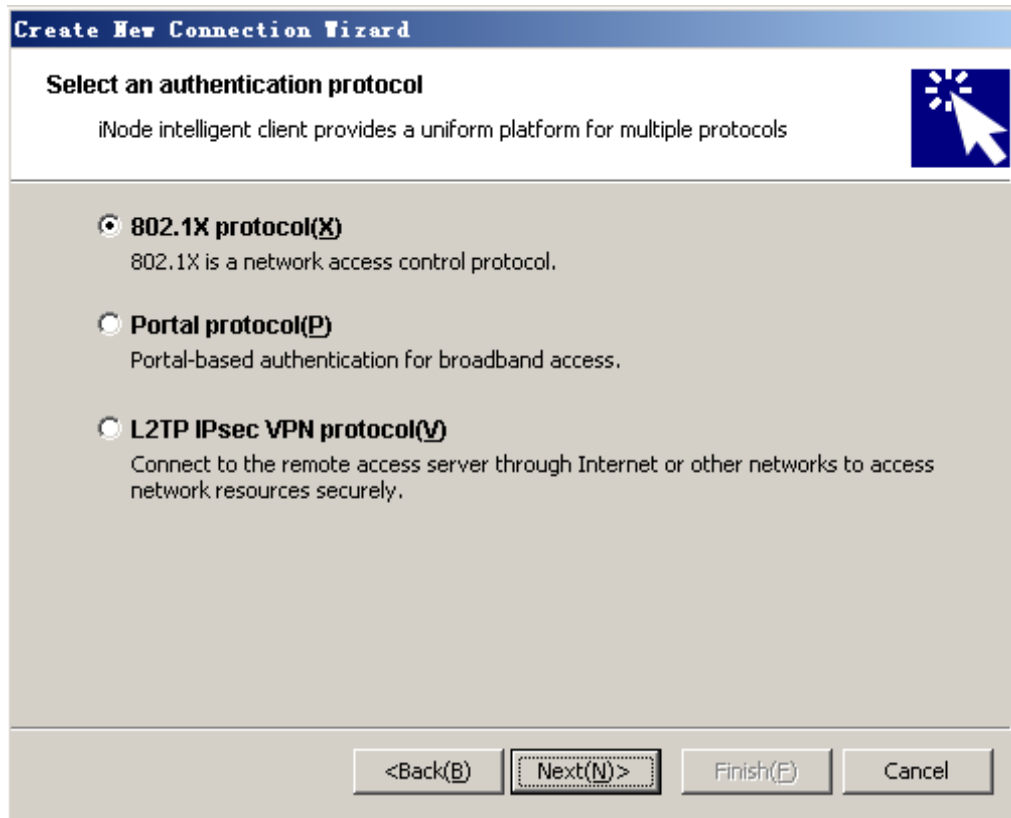
1. Open the iNode client as shown in Figure 2.

Figure 2 Opening iNode client



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

Figure 3 Creating a new connection



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

Figure 4 Configuring the connection name, username, and password

Create New Connection Wizard

Account Information

Input user name and password for network access, and certificate in order to enhance communication security.

Connection name(C):

Username(U):

Password(P):

Save username and password(Y)

Domain(D):

Enable advanced authentication(E)

MAC authentication(M)

Smart Card authentication(K)

Certificate authentication(I)

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

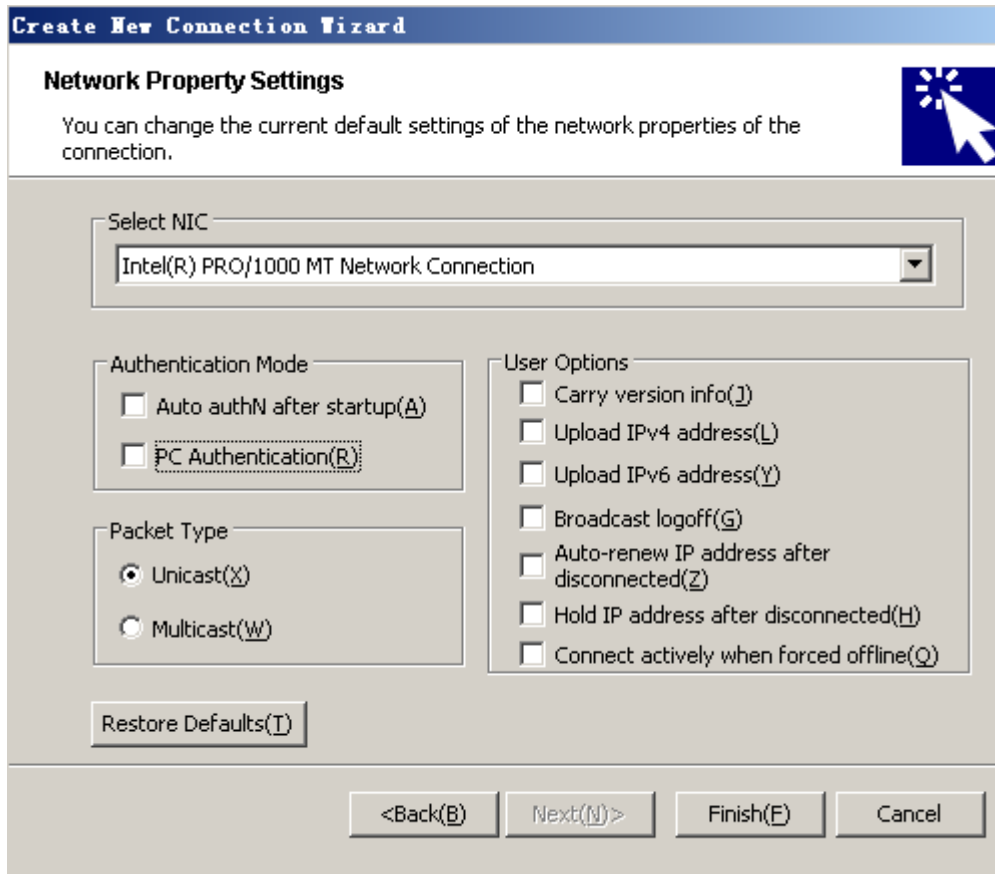
- Username specified on the iNode client.
- Domain and username format configuration on the access device.
- Service suffix on UAM.

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 connection properties.

Figure 5 Configuring 802.1X connection properties

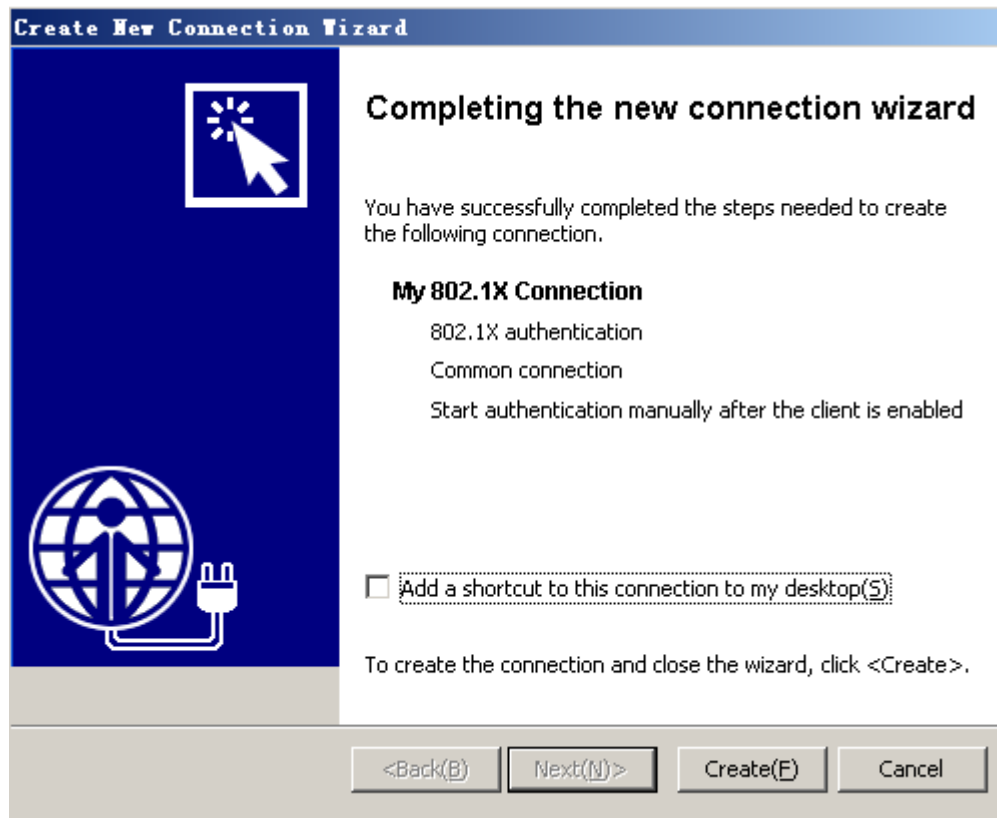


If you select the **Carry version info(J)** item in the **User Options** area, the 802.1X client adds the client version number to the EAP packets that are sent to the UAM for 802.1X authentication. If you do not select this item, the 802.1X client sends standard EAP packets to the UAM for 802.1X authentication.

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

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

Figure 6 Completing the new connection wizard



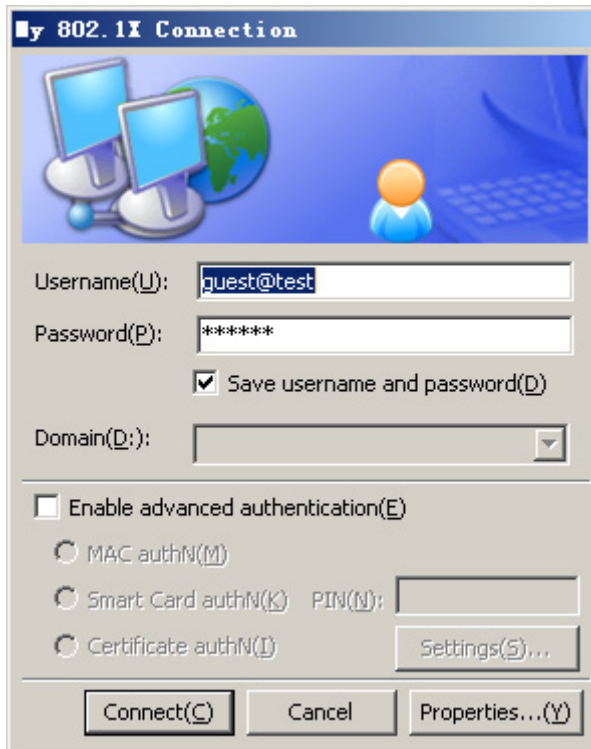
Verifying the configuration

Verify that the user can pass authentication and access the network:

Click **Connect** on the iNode client to initiate the connection.

On the **My 802.1X Connection** window, enter username **guest@test** and password **123456**, and then click **Connect(C)**.

Figure 7 Initiating the 802.1X connection



Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A (the access device):

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

```

interface Vlan-interface11
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 11
#

```

- Switch B (the RADIUS server):

```

#
radius-server client-ip 10.1.1.2 key cipher $c$3$EEKWoSNy6Om3tZ0PhUbTPLuWMy2+aw==
#
radius-server user guest
 password cipher $c$3$4rJuGA/vjrZHO+o33+/NPkcVZWuY8nnDzw==
#
interface Vlan-interface11
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/10
 port access vlan 11
#

```

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

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

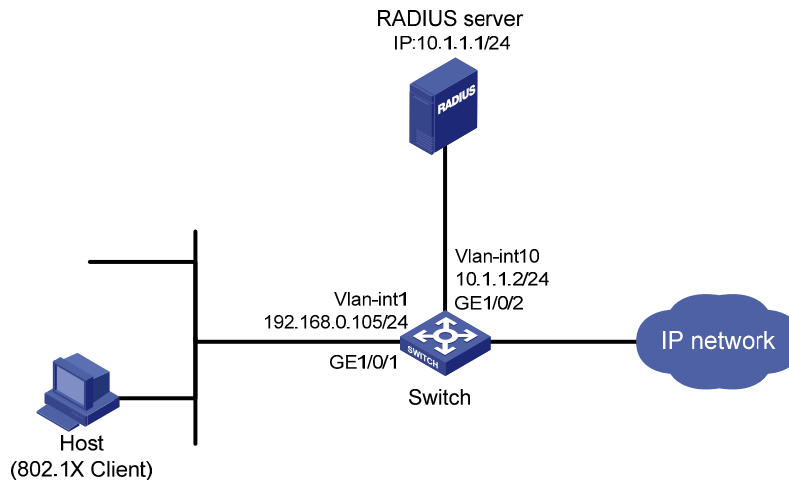
Network requirements

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. IMC runs on the RADIUS server.

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

Figure 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 different 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

The screenshot shows two windows from the IMC interface. The top window, titled 'Basic Information', contains the following fields and options:

- Service Name:** service1
- Service Suffix:** test
- Service Group:** Ungrouped
- Default Access Rule:** default
- Default Proprietary Attribute Assignment Policy:** Do not use
- Description:** (empty text box)
- Available:**
- Portal Fast Authentication on Endpoints:**

The bottom window, titled 'Access Policy List', features an 'Add' button and a table with the following columns: Access Scenario, Access Rule, Proprietary Attribute Assignment Policy, Priority, Modify, and Delete.

At the bottom of the interface are 'OK' and 'Cancel' buttons.

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:
 - 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

The screenshot shows the 'Add Access User' configuration page in IMC. The breadcrumb path is 'User >> All Access Users >> Add Access User'. The page is divided into two main sections: 'Access Information' and 'Access Service'.

Access Information:

- User Name:** user1 (with 'Select' and 'Add User' buttons)
- Account Name:** guest
- Options:** Trial Account, Default BYOD User, Computer User, Fast Access User (all unchecked).
- Password:** (masked with dots) and **Confirm Password:** (masked with dots).
- Other Options:** Allow User to Change Password (checked), Enable Password Strategy (unchecked), Modify Password at Next Login (checked).
- Expiration Date:** (calendar icon)
- Max. Idle Time:** (text box) Minutes
- Max. Smart Terminal Bindings for Portal:** 1
- Max. Concurrent Logins:** 1
- Login Message:** (text box)

Access Service:

	Service Name	Service Suffix	Status	Allocate IP
<input checked="" type="checkbox"/>	service1	test	Available	

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.
[Switch-radius-radius1] key authentication aabbcc
# Configure the RADIUS server type as extended.
[Switch-radius-radius1] server-type extended
# Set the response timeout time of the RADIUS server to 5 seconds. Set the maximum number of RADIUS
packet retransmission attempts to 5.
[Switch-radius-radius1] timer response-timeout 5
[Switch-radius-radius1] retry 5
[Switch-radius-radius1] quit
# Create an ISP domain named test and enter ISP domain view.
[Switch] domain test
# 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
# Enable the idle cut function, and set the idle timeout period to 20 minutes.
[Switch-isp-test] idle-cut enable 20
[Switch-isp-test] quit
# Specify domain test as the default ISP domain.
[Switch] domain default enable test
# Enable 802.1X on port GigabitEthernet 1/0/1.
[Switch] interface gigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] quit
# Configure port GigabitEthernet 1/0/1 to implement MAC-based access control. By default, the port
implements MAC-based access control.
[Switch] dot1x port-method macbased interface gigabitEthernet 1/0/1
# Enable 802.1X globally.
[Switch] dot1x

```

Configuring the 802.1X client

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 the user can pass 802.1X authentication and access the Internet:

Click **Connect** on the iNode client.

On the **My 802.1X Connection** window, enter username **guest@test** and password **123456**, and then click **Connect(C)**.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
 domain default enable test
#
 dot1x
#
vlan 1
#
radius scheme radius1
 server-type extended
 primary authentication 10.1.1.1
 key authentication cipher $c$3$LAV0oGNAM9Z/CuVcWONBH4xezu48Agh5aQ==
 timer response-timeout 5
 retry 5
#
domain test
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 access-limit disable
 state active
 idle-cut enable 20 10240
 self-service-url disable
#
interface Vlan-interface10
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
#
```

Example: Configuring 802.1X unicast trigger

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

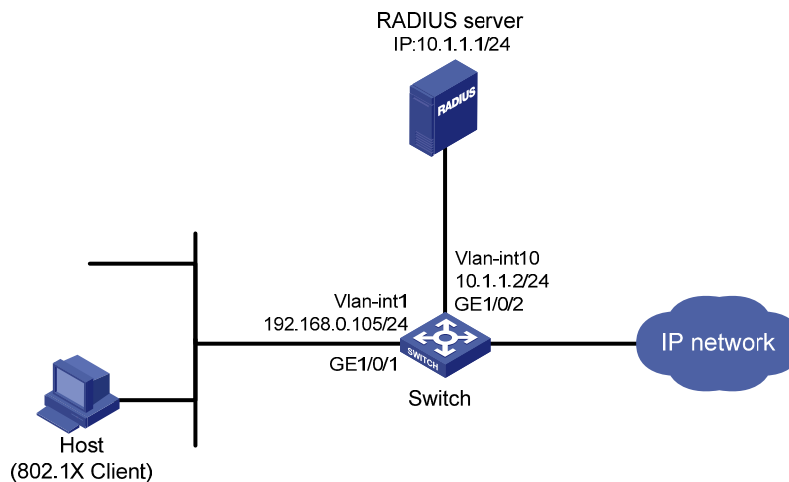
Network requirements

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 meet the following requirements:

- 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.

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. To ensure system performance, HP recommends that you disable the 802.1X multicast trigger function and enable the unicast trigger function.

Configuration procedures

Configuring interfaces

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

Configuring the RADIUS server

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.
[Switch-radius-radius1] key authentication aabbcc

# Configure the RADIUS server type as extended.
[Switch-radius-radius1] server-type extended
[Switch-radius-radius1] quit

# Create ISP domain test and enter ISP domain view.
[Switch] domain test

# Configure ISP domain test to use RADIUS scheme radius1 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 GigabitEthernet 1/0/1.
[Switch] interface gigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo dot1x multicast-trigger

# Enable the 802.1X unicast trigger function on the port.
[Switch-GigabitEthernet 1/0/1] dot1x unicast-trigger

# Enable 802.1X on the port.
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] quit

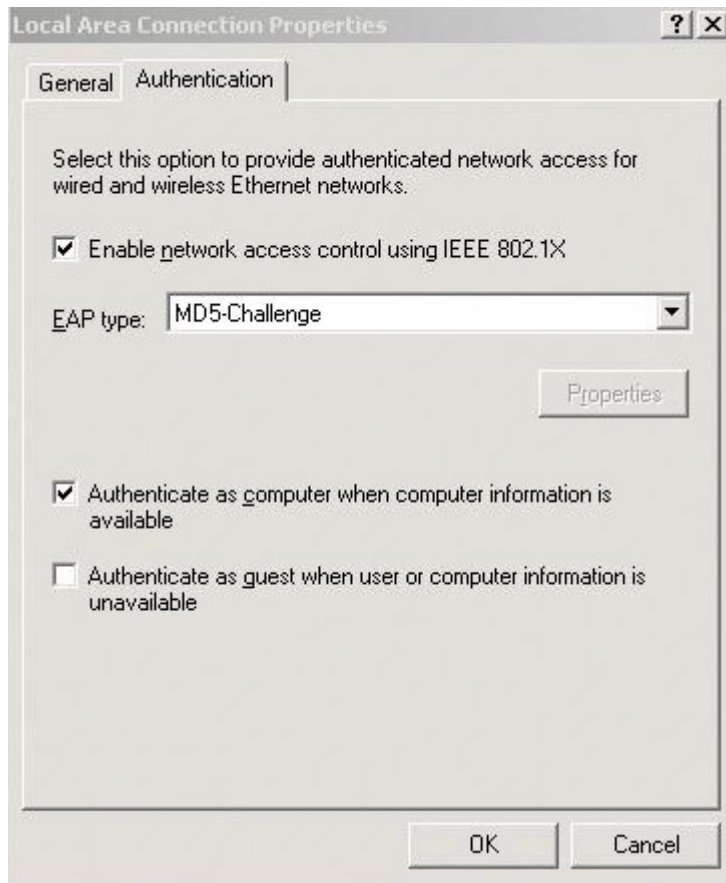
# Configure the port to implement MAC-based access control. By default, the port implements MAC-based access control.
[Switch] dot1x port-method macbased interface gigabitEthernet 1/0/1

# Enable 802.1X globally.
[Switch] dot1x
```

Configuring the 802.1X client

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

Figure 14 Enabling 802.1X authentication for the Windows XP system



Verifying the configuration

Verify that the user can pass authentication and access the Internet:

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

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
domain default enable test
#
dot1x
#
radius scheme radius1
server-type extended
primary authentication 10.1.1.1
key authentication $c$3$LAV0oGNAM9Z/CuVcWONBH4xezu48Agh5aQ==
#
```

```

domain test
 authentication default radius-scheme radius1
 authorization default radius-scheme radius1
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 undo dot1x multicast-trigger
 dot1x
 dot1x unicast-trigger
#

```

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

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

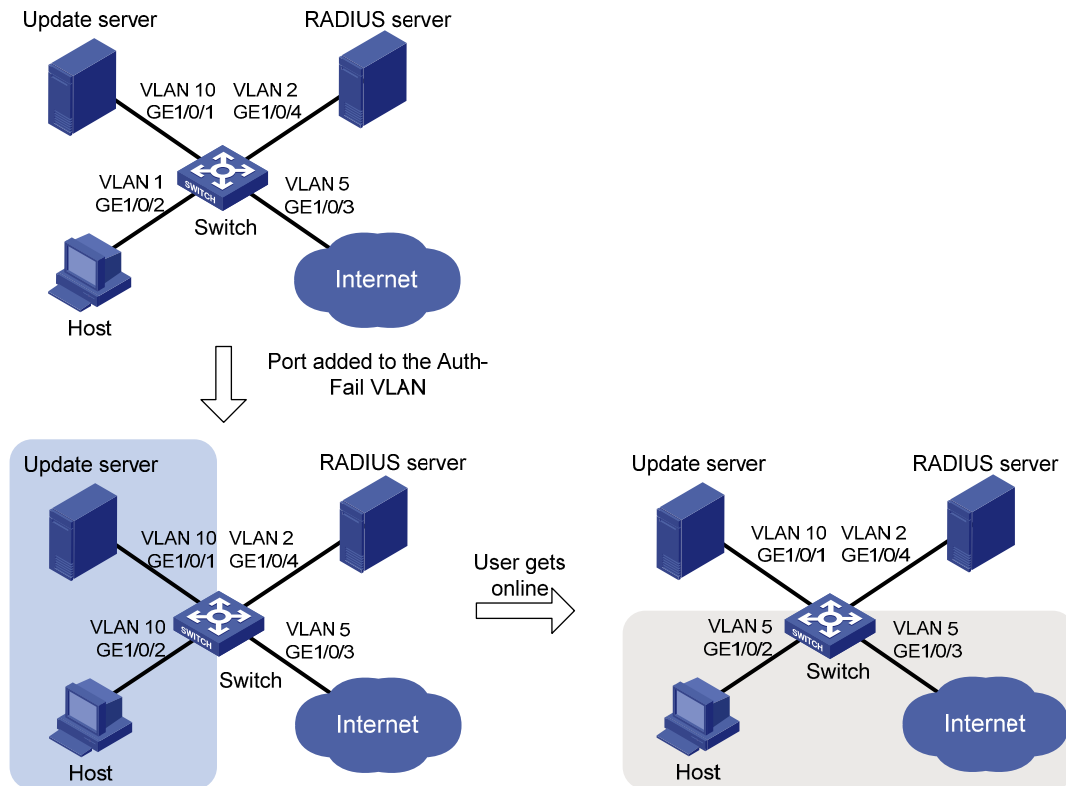
Network requirements

As shown in [Figure 15](#), users on the host must pass 802.1X authentication to access the Internet.

Configure the switch to meet the following requirements:

- Use the RADIUS server to provide authentication and authorization services for the users.
- Assign GigabitEthernet 1/0/2 to VLAN 10 after the user fails 802.1X authentication. The user can visit the update server in VLAN 10 to download and upgrade software.
- Assign GigabitEthernet 1/0/2 to VLAN 5 after the user passes 802.1X authentication. The user can access the Internet.

Figure 15 Network diagram



Requirements analysis

To assign GigabitEthernet 1/0/2 to VLAN 10 after the user fails authentication, you must configure VLAN 10 as the 802.1X Auth-Fail VLAN on GigabitEthernet 1/0/2.

To assign GigabitEthernet 1/0/2 to VLAN 5 after the user passes authentication, you must specify VLAN 5 as the authorization VLAN on the RADIUS server.

Configuration restrictions and guidelines

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

- Assign different IDs to the voice VLAN, the port VLAN, and the 802.1X Auth-Fail VLAN on a port, so the port can correctly process VLAN tagged incoming traffic.
- You cannot specify a VLAN as both a super VLAN and an 802.1X Auth-Fail VLAN.

Configuration procedures

Configuring the RADIUS server

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

To add an access rule:

1. Click the **Service** tab.

2. From the navigation tree, select **User Access Manager > Access Rule Management**.
3. Click **Add**.
4. Select **Deploy VLAN**, and enter the VLAN number.

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

Figure 16 Authorizing a VLAN to authenticated users

5. Click **OK**.

Configuring the switch

1. Configure VLANs:

Assign port GigabitEthernet 1/0/2 to VLAN 1.

```
<Switch> system-view
[Switch] vlan 1
[Switch-vlan1] port gigabitethernet 1/0/2
[Switch-vlan1] quit
```

Create VLAN 10 and assign GigabitEthernet 1/0/1 to VLAN 10.

```
[Switch] vlan 10
[Switch-vlan10] port gigabitethernet 1/0/1
[Switch-vlan10] quit
```

Create VLAN 2 and assign GigabitEthernet 1/0/4 to VLAN 2.

```
[Switch] vlan 2
[Switch-vlan2] port gigabitethernet 1/0/4
[Switch-vlan2] quit
```

Create VLAN 5 and assign GigabitEthernet 1/0/3 to VLAN 5.

```
[Switch] vlan 5
[Switch-vlan5] port gigabitethernet 1/0/3
[Switch-vlan5] quit
```

2. Configure the RADIUS scheme:

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

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

Specify the RADIUS server at **10.11.1.1** as the primary authentication server. Set the authentication port to **1812**.

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

Configure the shared key to **aabbcc** for secure RADIUS communication.

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

Configure the RADIUS server type as **extended**.

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

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

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

3. Configure the ISP domain:

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

```
[Switch] 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
```

4. Configure 802.1X:

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

```
[Switch] interface gigabitethernet 1/0/2
```

```
[Switch-GigabitEthernet1/0/2] dot1x
```

Configure the port to implement port-based access control.

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

Set the authorization state of the port to **auto**. By default, the authorization state of the port is **auto**.

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

Configure VLAN 10 as the Auth-Fail VLAN for GigabitEthernet 1/0/2.

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

```
[Switch-GigabitEthernet1/0/2] quit
```

Enable 802.1X globally.

```
[Switch] dot1x
```

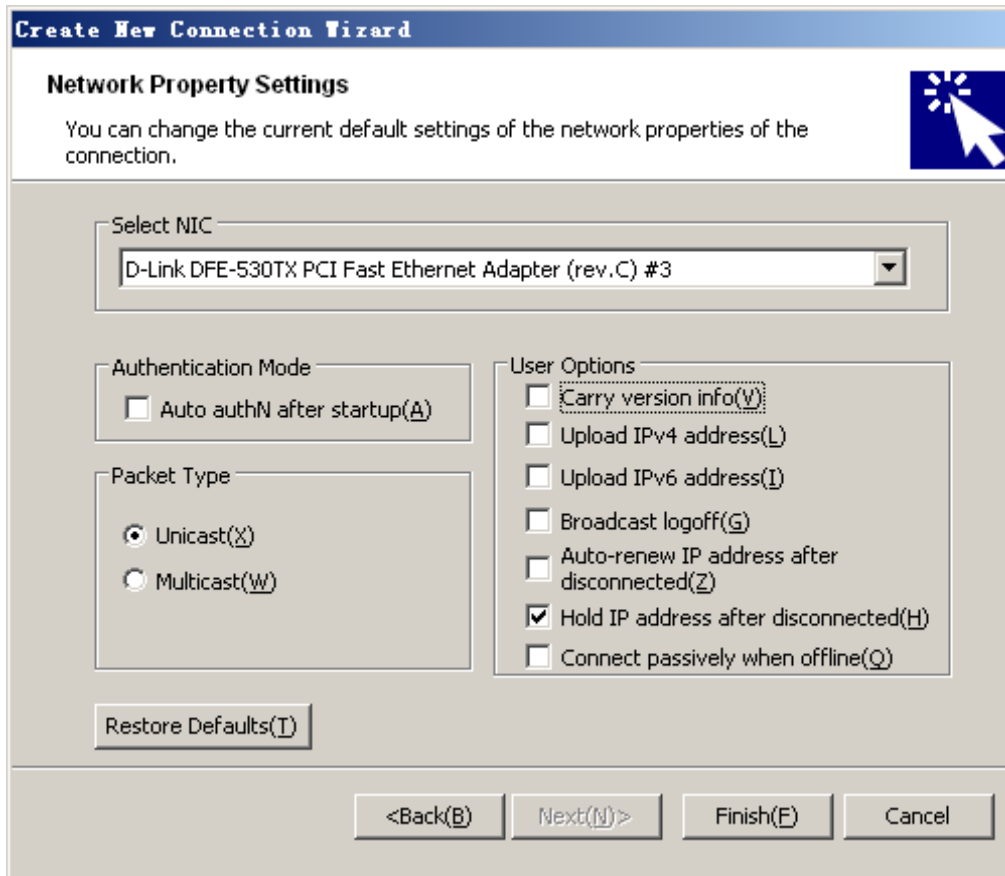
Configuring the 802.1X client

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

To set 802.1X network properties:

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

Figure 17 Configuring 802.1X network property settings



Verifying the configuration

Use the **display dot1x interface gigabitethernet 1/0/2** command to verify the 802.1X Auth-Fail VLAN configuration on port GigabitEthernet 1/0/2.

After a user fails to pass 802.1X authentication on the port, use the **display vlan 10** command to verify whether GigabitEthernet 1/0/2 is assigned to VLAN 10.

After the user passes authentication, use the **display interface gigabitethernet 1/0/2** command to verify that port GigabitEthernet 1/0/2 has been assigned to VLAN 5.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

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

```

#
vlan 5
#
vlan 10
#
radius scheme radius1
  server-type extended
  primary authentication 10.1.1.1
  key authentication cipher $c$3$LAV0oGNAM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain test
  authentication lan-access radius-scheme radius1
  authorization lan-access radius-scheme radius1
  access-limit disable
  state active
  idle-cut disable
  self-service-url disable
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port access vlan 10
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  dot1x auth-fail vlan 10
  dot1x port-method portbased
  dot1x
#
interface GigabitEthernet1/0/3
  port link-mode bridge
  port access vlan 5
#
interface GigabitEthernet1/0/4
  port link-mode bridge
  port access vlan 2
#

```

Example: Configuring 802.1X authentication with ACL assignment

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

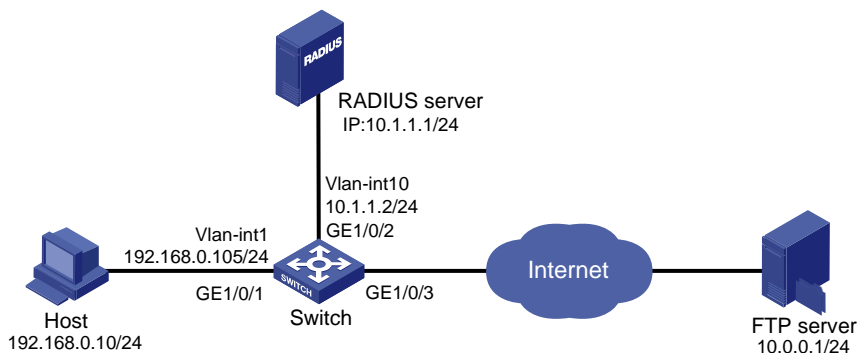
Network requirements

As shown in [Figure 18](#):

- The host must pass 802.1X authentication to access the Internet.
- A RADIUS server is available for authentication and authorization of 802.1X users.

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

Figure 18 Network diagram



Configuration restrictions and guidelines

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

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

Configuration procedures

Configuring IP addresses

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

Configuring the RADIUS server

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

To add an access rule:

1. Click the **Service** tab.
2. From the navigation tree, select **User Access Manager > Access Rule Management**.
3. Click **Add**.

- In the **Authorization Information** area, select **Deploy ACL** and **Add Manually**, and enter the ACL number.

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

Figure 19 Deploying an ACL

- Click **OK**.

Configuring the switch

- Configure the RADIUS scheme:

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 1812
```

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

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

Configure the RADIUS server type as **extended**.

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

Configure the device to send usernames with domain suffix.

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

- Configure AAA:

Create ISP domain **test**.

```
[Switch] domain test
```

Configure the domain 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 for 802.1X authentication.

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

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

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

- Configure 802.1X:

Set the periodic re-authentication timer to 1800 seconds.

```

[Switch] dot1x timer reauth-period 1800
# Enable the 802.1X periodic online user re-authentication function on port GigabitEthernet
1/0/1.
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x re-authenticate
# Enable 802.1X on GigabitEthernet 1/0/1.
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] quit
# Enable 802.1X globally.
[Switch] dot1x

```

Verifying the configuration

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

```
C:\>ping 10.0.0.1
```

```
Pinging 10.0.0.1 with 32 bytes of data:
```

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

```
Ping statistics for 10.0.0.1:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```

#
domain default enable test
#
dot1x
dot1x timer reauth-period 1800
#
acl number 3000
rule 0 deny ip destination 10.0.0.1 0
#
radius scheme radius1
server-type extended
primary authentication 10.1.1.1
key authentication cipher $c$3$LAV0oGNAM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain test
authentication lan-access radius-scheme radius1
authorization lan-access radius-scheme radius1

```

```

access-limit disable
state active
idle-cut disable
self-service-url disable
#
interface Vlan-interface10
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 dot1x re-authenticate
 dot1x
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
#

```

Example: Configuring EAD fast deployment

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

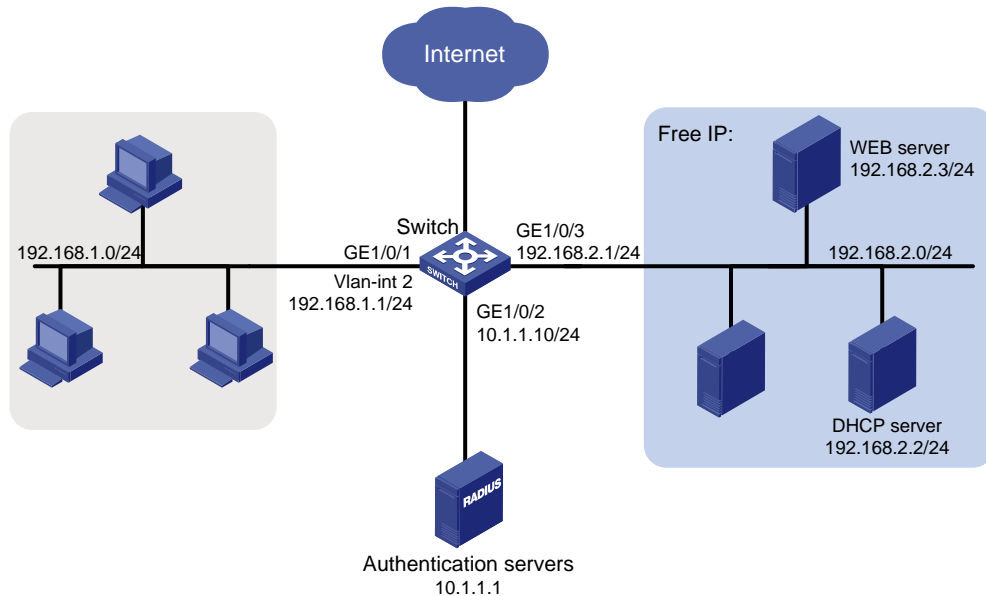
As shown in [Figure 20](#):

- The hosts on the intranet 192.168.1.0/24 are attached to port GigabitEthernet 1/0/1 of the switch (the network access device). They use DHCP to obtain IP addresses.
- A DHCP server and a Web server are deployed on the 192.168.2.0/24 subnet for users to obtain IP addresses and download client software.

Deploy an EAD solution for the intranet to control network access as follows:

- Allow unauthenticated users to visit the Web server and DHCP server. These users can obtain IP addresses on the segment of 192.168.1.0/24 through DHCP.
- Redirect unauthenticated users to a preconfigured webpage when the users use a Web browser to access any external network except 192.168.2.0/24. The webpage allows users to download the 802.1X client.
- Allow authenticated 802.1X users to access the network.

Figure 20 Network diagram



Configuration restrictions and guidelines

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

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

Configuration procedures

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

Enable DHCP.

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

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

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

Enable the relay agent on VLAN-interface 2.

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

Correlate VLAN-interface 2 to the DHCP server group.

```
[Switch-Vlan-interface2] dhcp relay server-select 1  
[Switch-Vlan-interface2] quit
```

3. Configure the RADIUS scheme and ISP domain in the same way the RADIUS scheme and ISP domain are configured in "[Example: Configuring RADIUS-based 802.1X authentication \(IMC server\)](#)."

4. Configure 802.1X:

```
# Configure the free IP.
[Switch] dot1x free-ip 192.168.2.0 24
# Configure the redirect URL for client software download.
[Switch] dot1x url http://192.168.2.3
# Enable 802.1X on port GigabitEthernet 1/0/1.
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] quit
# Enable 802.1X globally.
[Switch] dot1x
```

Verifying the configuration

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

```
C:\>ping 192.168.2.3
```

```
Pinging 192.168.2.3 with 32 bytes of data:
```

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

```
Ping statistics for 192.168.2.3:
```

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

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

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
domain default enable test
#
dhcp relay server-group 1 ip 192.168.2.2
#
dot1x
dot1x url http://192.168.2.3
dot1x free-ip 192.168.2.0 255.255.255.0
#
```



```
radius scheme radius1
  server-type extended
  primary authentication 10.1.1.1
  key authentication cipher $c$3$LAV0oGNaM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain test
  authentication lan-access radius-scheme radius1
  authorization lan-access radius-scheme radius1
  access-limit disable
  state active
  idle-cut disable
  self-service-url disable
#
interface Vlan-interface2
  ip address 192.168.1.1 255.255.255.0
  dhcp select relay
  dhcp relay server-select 1
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  dot1x
#
```

AAA configuration examples

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

Example: Configuring local authentication and authorization for FTP users

Applicable product matrix

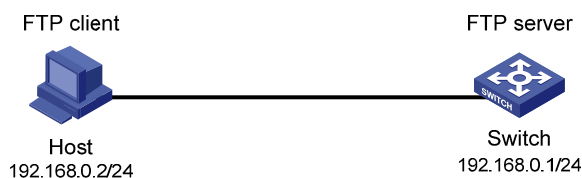
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 21](#), users on the host can access the switch through FTP.

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

Figure 21 Network diagram



Configuration restrictions and guidelines

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

- By default, the switch uses the default ISP domain named **system**.
- When you configure the default ISP domain, make sure the specified domain exists. All users whose usernames do not include domain names are authenticated in the default ISP domain.
- The switch selects the ISP domain for user authentication in the following order:
 - a. ISP domain specified for authentication by the access module such as 802.1X, portal, and MAC authentication.

- b. ISP domain included in the username.
- c. Default ISP domain.

Configuration procedures

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

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

Enable the FTP server function.

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

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

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

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

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

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

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

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

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

Verifying the configuration

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

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

Configuration files

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

Example: Configuring RADIUS authentication and authorization for Telnet users

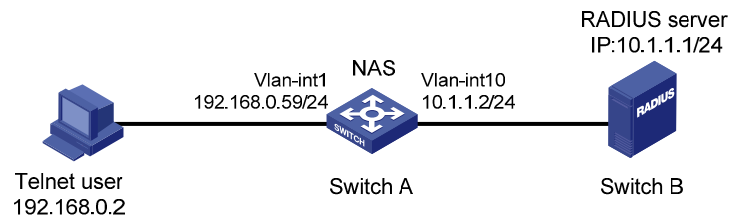
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 22](#), configure the NAS (Switch A) to implement RADIUS authentication and authorization for Telnet users.

Figure 22 Network diagram



Configuration restrictions and guidelines

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

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

Configuration procedures

Configuring interfaces

Configure the IP addresses for interfaces as shown in [Figure 22](#), and make sure the Telnet user, RADIUS server, and NAS can reach each other.

Configuring the NAS

Enable the Telnet server function.

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

Configure the switch to use AAA for Telnet users.

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

Create a RADIUS scheme named **rad**.

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

Configure the server at **10.1.1.1** as the primary RADIUS authentication server. Specify the authentication port as **1645**. Set the shared key to **abc** for secure RADIUS communication.

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

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

```

[SwitchA-radius-rad] user-name-format without-domain
# Specify the source IP address for outgoing RADIUS packets as 10.1.1.2.
[SwitchA-radius-rad] nas-ip 10.1.1.2

# Set the RADIUS server type to standard.
[SwitchA-radius-rad] server-type standard
[SwitchA-radius-rad] quit

# Create an ISP domain named domain1.
[SwitchA] domain domain1

# Configure the switch to use RADIUS scheme rad as the authentication method for login users in the ISP domain. Use local authentication as the backup authentication method.
[SwitchA-isp-domain1] authentication login radius-scheme rad local

# Configure the switch to use RADIUS scheme rad as the authorization method for login users in the ISP domain. Use local authentication as the backup authorization method.
[SwitchA-isp-domain1] authorization login radius-scheme rad local

# Configure the accounting method for login users as none.
[SwitchA-isp-domain1] accounting login none
[SwitchA-isp-domain1] quit

# Configure domain1 as the system default ISP domain.
[SwitchA] domain default enable domain1

# Create a local user named telnet1, and configure the Telnet service type and plaintext password 123456 for the user.
[SwitchA] local-user telnet1
[SwitchA-luser-telnet1] service-type telnet
[SwitchA-luser-telnet1] password simple 123456
[SwitchA-luser-telnet1] quit

```

Configuring the RADIUS server

```

# Create a local user named telnet1.
<SwitchB> system-view
[SwitchB] radius-server user telnet1

# Set the user's password to 123456 in plain text, which is the same as the password configured on Switch A.
[SwitchB-rdsuser-telnet1] password simple 123456
[SwitchB-rdsuser-telnet1] quit

# Configure the IP address of the RADIUS client as 10.1.1.2 and the shared key is abc in plain text.
[SwitchB] radius-server client-ip 10.1.1.2 key simple abc

```

Verifying the configuration

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

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

Login authentication

Username:telnet1@domain1

Password:

<SwitchA>

Display connection information on Switch A.

<SwitchA> display connection

Slot: 1

Index=1 ,Username=telnet1@domain1

IP=192.168.0.2

IPv6=N/A

Total 1 connection(s) matched on slot 1.

Total 1 connection(s) matched.

Configuration files

- The NAS:

```
#
telnet server enable
#
radius scheme rad
primary authentication 10.1.1.1 1645 key cipher
$c$3$A5ng5y1DclDYJiLkhovxImB09cAe3w==
user-name-format without-domain
nas-ip 10.1.1.2
#
domain domain1
authentication login radius-scheme rad local
authorization login radius-scheme rad local
accounting login none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
local-user telnet1
password cipher $c$3$albKG13b86oIxlt+U1YIbKe9R4fJufa35Q==
service-type telnet
```

```
#
user-interface vty 0 15
 authentication-mode scheme
#
```

- The RADIUS server:

```
#
radius-server client-ip 10.1.1.2 key cipher $c$3$EEKWoSNy6Om3tZ0PhUbTPLuWMy2+aw==
#
radius-server user telnet1
 password cipher $c$3$4rJuGA/vjrZHO+o33+/NPkcVZWuY8nnDzw==
#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0
#
```

Example: Configuring RADIUS authentication and authorization for SSH users

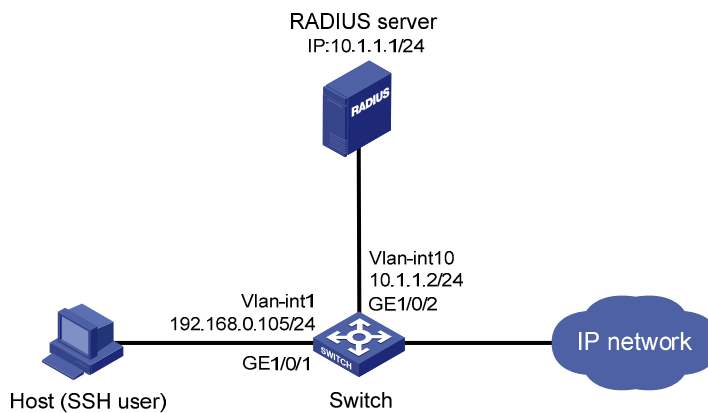
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 23](#), configure the switch to implement RADIUS authentication and authorization for SSH users.

Figure 23 Network diagram



Requirements analysis

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 command level.

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

Configuration restrictions and guidelines

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

Configuration procedures

Configuring interfaces

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

Configuring the RADIUS server

1. Add the switch to IMC as an access device:
 - a. Click the **Service** tab.
 - 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.
 - 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 24 Adding an access device in IMC

Service >> User Access Manager >> Access Device Management >> Access Device >> Add Access Device Help

Access Configuration

* Authentication Port	1812	* Accounting Port	1813
* Shared Key	*****	* Confirm Shared Key	*****
Access Area	-	Service Type	Device Management Service
Access Device Type	HP(General)	RADIUS Accounting	Fully Supported
Service Group	Ungrouped		

Device List

Select Add Manually Clear All

Total Items: 1.

Device Name	Device IP	Device Model	Comments	Delete
	10.1.1.2			

OK Cancel

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.
 - Select **3** from the **EXEC Priority** list.
 - 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 25 Adding a device management user account in IMC

User >> Device Management User >> Add Device Management User

Add Device Management User

Basic Information of Device Management User

- * Account Name: hello@bbb
- * User Password: [masked]
- * Confirm Password: [masked]
- Service Type: SSH
- EXEC Priority: 3
- Role Name: [empty]

Tips
Note: If you enter multiple role names, enter one role name on each line. The sum of the total number of bytes occupied by the role names and the number of role names (excluding duplicate names) cannot exceed 234. For example, if you enter 10 role names, the number of bytes occupied by the role names cannot exceed 224.

Bound User IP List

Add Delete

Total Items: 0.

Start IP	End IP	Delete

IP Address List of Managed Devices

Add Delete

Total Items: 1.

Start IP	End IP	Delete
<input type="checkbox"/> 10.1.1.2	10.1.1.2	<input type="checkbox"/>

OK Cancel

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 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 and DSA key pairs and enable the SSH server.

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

```

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

# Configure the switch to use AAA for SSH users.
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
[Switch-ui-vty0-15] protocol inbound ssh
[Switch-ui-vty0-15] quit

# Create a RADIUS scheme named rad.
[Switch] radius scheme rad
New Radius scheme

# Configure the primary authentication server with IP address 10.1.1.1 and authentication port number 1812.
[Switch-radius-rad] primary authentication 10.1.1.1 1812

# Set the shared key for secure RADIUS authentication communication to aabbcc.
[Switch-radius-rad] key authentication aabbcc

# Configure the switch to include the domain name in usernames to be sent to the RADIUS server.
[Switch-radius-rad] user-name-format with-domain

# Configure the RADIUS server type, which must be extended for IMC.
[Switch-radius-rad] server-type extended
[Switch-radius-rad] quit

# Configure the authentication and authorization methods for login users in ISP domain bbb.
[Switch] domain bbb
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] quit

```

Configuring the host

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

Verifying the configuration

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

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

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

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

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
vlan 10
#
radius scheme rad
server-type extended
primary authentication 10.1.1.1
key authentication cipher $c$3$LAV0oGNAM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain bbb
authentication login radius-scheme rad
authorization login radius-scheme rad
access-limit disable
state active
idle-cut disable
self-service-url disable
#
interface Vlan-interface1
ip address 192.168.0.105 255.255.255.0
#
interface Vlan-interface10
ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 10
#
ssh server enable
#
```

```

user-interface vty 0 15
 authentication-mode scheme
 protocol inbound ssh
#

```

Example: Configuring RADIUS authentication and authorization for different user types

Applicable product matrix

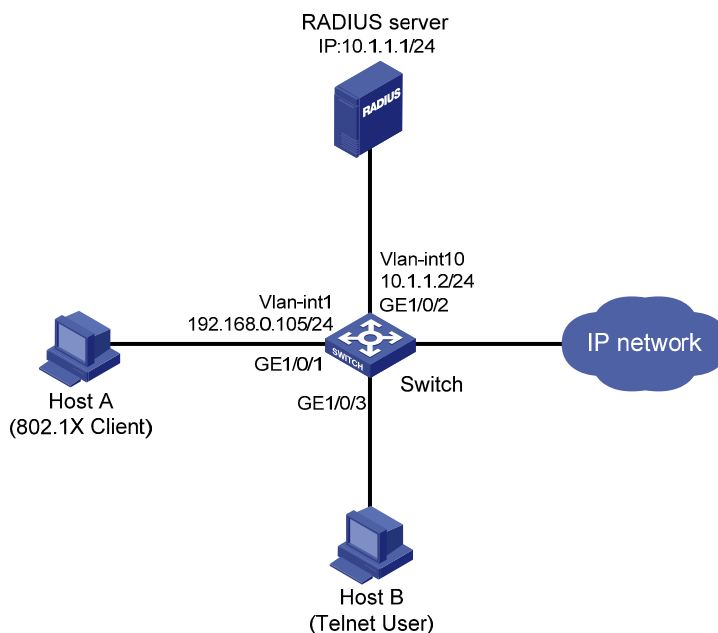
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 26](#), the RADIUS server runs on IMC to provide authentication and authorization. Configure the switch to complete the following functions:

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

Figure 26 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 different IMC versions, deployed service components, and UAM system settings. For more information, see *HP IMC User Access Manager Administrator Guide*.

Configuration procedures

Configuring interfaces

Configure the IP addresses for interfaces as shown in [Figure 26](#), and make sure the hosts, server, and switch can reach each other.

Configuring the RADIUS server

1. Add the switch to IMC as an access device:
 - a. Click the **Service** tab.
 - 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 **LAN Access Service** from the **Service Type** list.
 - Select **HP(General)** from the **Access Device Type** list.
 - 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 27 Adding an access device in IMC

Service >> User Access Manager >> Access Device Management >> Access Device >> Add Access Device Help

Access Configuration			
* Authentication Port	1812	* Accounting Port	1813
* Shared Key	*****	* Confirm Shared Key	*****
Access Area	—	Service Type	LAN Access Service
Access Device Type	HP(General)	RADIUS Accounting	Fully Supported
Service Group	Ungrouped		

Device List

Select Add Manually Clear All

Total Items: 1

Device Name	Device IP	Device Model	Comments	Delete
	10.1.1.2			X

OK Cancel

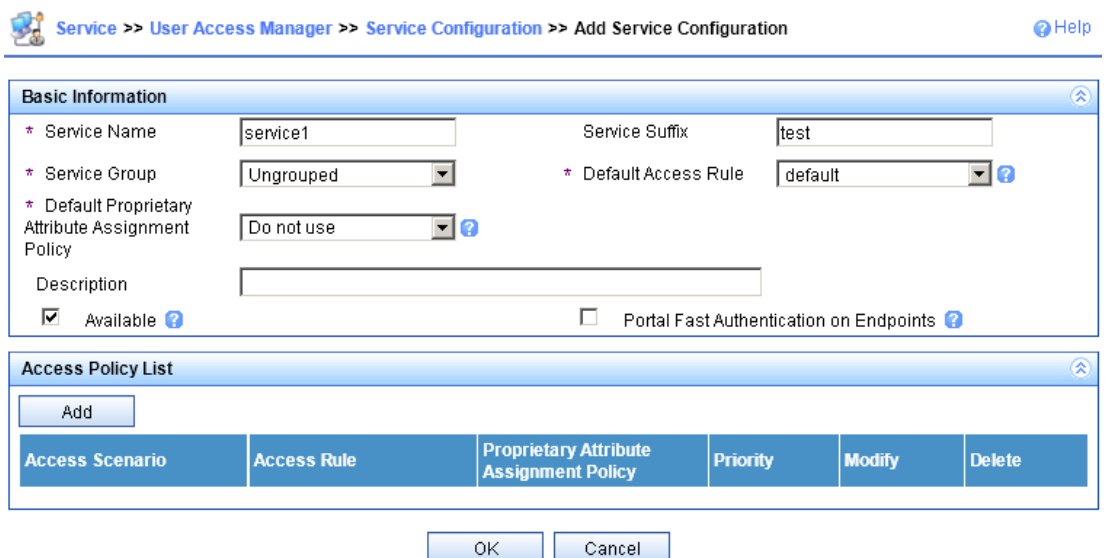
2. Create an access rule:
 - a. From the navigation tree, select **User Access Manager > Access Rule Management**.
 - b. Click **Add**.
 - c. Enter **default** in the **Access Rule Name** field and use the default settings for other parameters.
 - d. Click **OK**.

Figure 28 Adding an access rule in IMC



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

Figure 29 Adding a service in IMC



4. Create an access user account and assign the service to the account:
 - a. Click the **User** tab.

- b. From the navigation tree, select **User Access Manager > Access User View > All Access Users**.
- c. Click **Add**.
- d. In the **Access Information** area, configure the following parameters:
 - Click **Add User** to create a Platform user named **user1**.
 - Enter **guest** in the **Account Name** field to identify the 802.1X user.
 - Enter **123456** in **Password** and **Confirm Password** fields.
 - Use the default settings for other parameters.
- e. In the **Access Service** area, select **service1** on the list.
- f. Click **OK**.

Figure 30 Adding an access user account in IMC

User >> All Access Users >> Add Access User

Access account

Access Information

* User Name: user1 [Select] [Add User]
 * Account Name: guest
 Trial Account Default BYOD User Computer User Fast Access User
 * Password: 123456 * Confirm Password: 123456
 Allow User to Change Password Enable Password Strategy Modify Password at Next Login
 Expiration Date: [] [?] Max. Smart Terminal Bindings for Portal: 1 [?]
 Max. Idle Time: [] Minutes Max. Concurrent Logins: 1
 Login Message: []

Access Service

	Service Name	Service Suffix	Status	Allocate IP
<input checked="" type="checkbox"/>	service1	test	Available	

Configuring the switch

Enable the Telnet server function.

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

Configure the switch to use AAA for Telnet users.

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

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

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

Create a RADIUS scheme named **radius1**.

```
[Switch] radius scheme radius1
[Switch-radius-radius1] primary authentication 10.1.1.1 1812
```

```

[Switch-radius-radius1] key authentication aabbcc
[Switch-radius-radius1] server-type extended
[Switch-radius-radius1] quit

# Create an ISP domain named test.
[Switch] domain test

# Configure the ISP domain to use RADIUS scheme radius1 for the authentication of LAN users.
[Switch-isp-test] authentication lan-access radius-scheme radius1

# Implement local authentication for login users in the ISP domain.
[Switch-isp-test] authentication login local
[Switch-isp-test] quit

# Configure ISP domain test as the system default ISP domain.
[Switch] domain default enable test

# Enable 802.1X on interface GigabitEthernet 1/0/1.
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] quit

# Configure interface GigabitEthernet 1/0/1 to implement port-based access control. By default, the
port implements port-based access control.
[Switch] dot1x port-method macbased interface gigabitethernet 1/0/1

# Enable 802.1X globally.
[Switch] dot1x

```

Verifying the configuration

```

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

# Telnet to the switch from Host B, and enter the username telnet@test and password 123456. Verify that
the user can log in to the switch.

```

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```

#
domain default enable test
#
telnet server enable
#
dot1x
#
radius scheme radius1
server-type extended
primary authentication 10.1.1.1

```

```

key authentication cipher $c$3$LAV0oGNAM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain test
  authentication lan-access radius-scheme radius1
  authentication login local
  access-limit disable
  state active
  idle-cut disable
  self-service-url disable
#
local-user telnet
  password cipher $c$3$h9XubfNGPUajFnOqaj8bXlVgB3j1Ph+qRA==
  service-type telnet
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  dot1x
#
user-interface vty 0 15
  authentication-mode scheme
  protocol inbound telnet
#

```

Example: Configuring temporary user level authorization for Telnet users

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

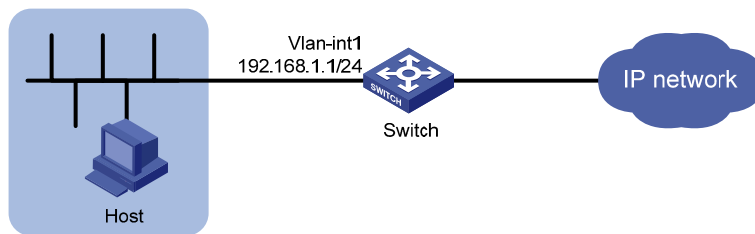
As shown in [Figure 31](#), users can Telnet to the switch.

Configure the switch to perform the following operations:

- Implement local authentication and authorization for Telnet users.
- Assign the level-1 user privilege level (monitor) to the login Telnet users. These users can access all level-1 commands for system maintenance and troubleshooting, including the **debugging** commands.

- Authorize the level-3 (manage) user privilege level temporarily to the login users without logging them out of the switch.

Figure 31 Network diagram



Requirements analysis

To perform local authentication and authorization, you must enable scheme (AAA) authentication for user interfaces on the switch and set the AAA method to **local**.

To assign the level-1 user privilege level to the login users, you must specify the user privilege level as 1 on the switch.

To authorize a user privilege level temporarily to the login users without logging them out of the switch, you must configure the following for the user privilege level:

- An authentication method. The local-only authentication method is configured in this example.
- A super password.

Configuration procedures

Assign an IP address to VLAN-interface 1, the Telnet user access interface.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.1 255.255.255.0
[Switch-Vlan-interface1] quit
```

Enable the Telnet server function.

```
[Switch] telnet server enable
```

Enable scheme authentication for 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 methods for login users. By default, the authentication and authorization methods are **local**.

```
[Switch-isp-bbb] authentication login local
```

```

[Switch-isp-bbb] authorization login local
[Switch-isp-bbb] quit

# Create local user test, specify its service type as Telnet, and set its password to 123456.
[Switch] local-user test
[Switch-luser-test] service-type telnet
[Switch-luser-test] password simple 123456

# Specify the user privilege level as 1 (monitor).
[Switch-luser-test] authorization-attribute level 1
[Switch-luser-test] quit

# Enable local-only authentication for the users to obtain a user privilege level temporarily without
reconnecting to the switch.
[Switch] super authentication-mode local

# Set super password localpass in plain text for changing the user privilege level temporarily to 3. By
default, the user privilege level for this command is 3.
[Switch] super password level 3 simple localpass

```

Verifying the configuration

Use username **test@bbb** and password **123456** to Telnet to the switch. Verify that the user can access all level-1 commands. The output varies with device models and software versions.

```
C:\>telnet 192.168.1.1
```

```

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

```

```
Login authentication
```

```
Username: test@bbb
```

```
Password: 123456
```

```
<Switch>?
```

```
User view commands:
```

```

 cfd          Connectivity fault detection (IEEE 802.1ag)
 cluster      Run cluster command
 debugging    Enable system debugging functions
 display      Display current system information
 graceful-restart Graceful restart
 ipc          Interprocess communication
 mcms         Specify multi-core multi-system configuration information
 moam         OAM function for MPLS-TP
 oam          OAM protocol

```

oap	Open application platform operation
packet	Packet commands
ping	Ping function
quit	Exit from current command view
refresh	Do soft reset
reset	Reset operation
screen-length	Specify the lines displayed on one screen
send	Send information to other user terminal interface
ssh2	Establish a secure shell client connection
super	Set the current user priority level
telnet	Establish one TELNET connection
terminal	Set the terminal line characteristics
tracert	Trace route function
undo	Cancel current setting

Change the user privilege level to 3 by entering super password **localpass**.

```
<Switch> super 3
```

Please input the password to change the privilege level. Press CTRL_C to abort.

```
 Password:
```

User privilege level is 3, and only those commands can be used whose level is equal or less than this.

Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE

The output shows that the Telnet user has obtained the level-3 user privilege level. The user can execute all level-3 commands.

Configuration files

```
#
super password level 3 cipher $c$3$S34PVJf2BXjuwDK4dBtL8qXhlCH5fC6g/B3ulQ==
#
telnet server enable
#
domain bbb
authentication login local
authorization login local
access-limit disable
state active
idle-cut disable
self-service-url disable
#
local-user test
password cipher $c$3$vUJAYBY38nmYwTftAMdn5HvryYWG/7Ti9Q==
authorization-attribute level 1
service-type telnet terminal
#
interface Vlan-interface1
ip address 192.168.1.1 255.255.255.0
```

```
#  
user-interface vty 0 15  
  authentication-mode scheme  
  user privilege level 3  
#
```

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 5500 EI & 5500 SI Switch Series ACL and QoS Configuration Guide*.

Example: Allowing a specific host to access the network

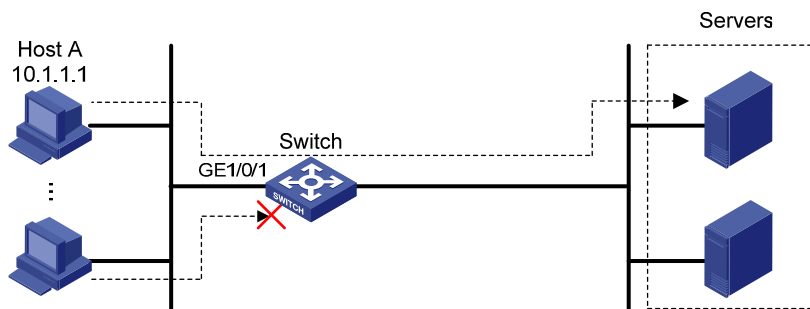
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

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

Figure 32 Network diagram



Requirements analysis

To implement time-based ACL rules, 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 two rules in the ACL. One rule permits packets sourced from 10.1.1.1 during working hours. The other rule denies packets sourced from any addresses 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] rule deny source any time-range working_time
[Switch-acl-basic-2000] quit
```

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

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

Verifying the configuration

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

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

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

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.

During a period outside of working hours, ping a server from any host. The server can be pinged successfully.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

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

Example: Denying a specific host to access the network

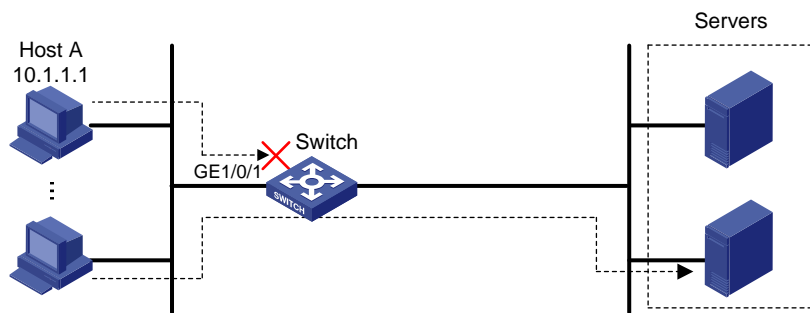
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 33](#), apply an ACL to GigabitEthernet 1/0/1 to deny packets sourced from Host A only during working hours (from 8:30 to 18:00) every day.

Figure 33 Network diagram



Requirements analysis

To implement time-based ACL rules, 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.

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

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

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

Verifying the configuration

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

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

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

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.

During a period outside of working hours, ping a server from any host. The server can be pinged successfully.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

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

Example: Allowing access between specific subnets

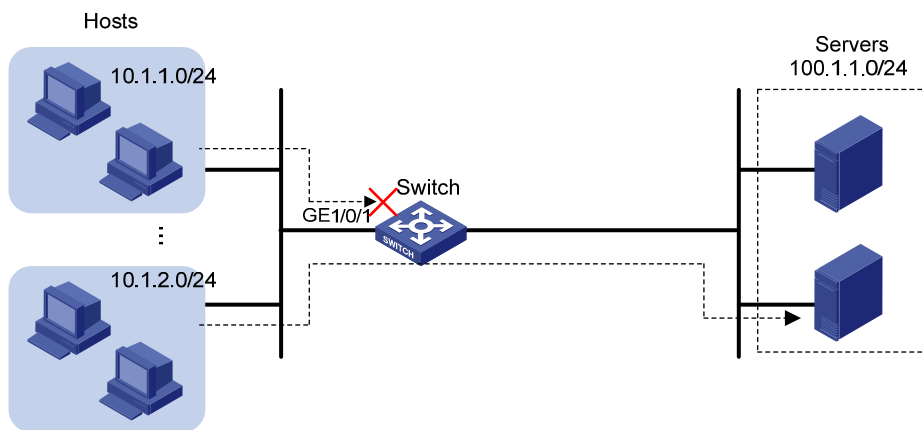
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 34](#), apply an ACL to allow only packets from 10.1.2.0/24 to 100.1.1.0/24.

Figure 34 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 and configure two rules in the ACL. One rule permits IP packets from 10.1.2.0/24 to 100.1.1.0/24. The other rule denies all 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 GigabitEthernet 1/0/1.

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

Verifying the configuration

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

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

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

Ping a server on subnet 100.1.1.0/24 from a host on subnet 10.1.2.0/24. The server can be pinged successfully.

Ping a server on subnet 100.1.1.0/24 from a host on another subnet. The server cannot be pinged.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

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

Example: Denying Telnet packets

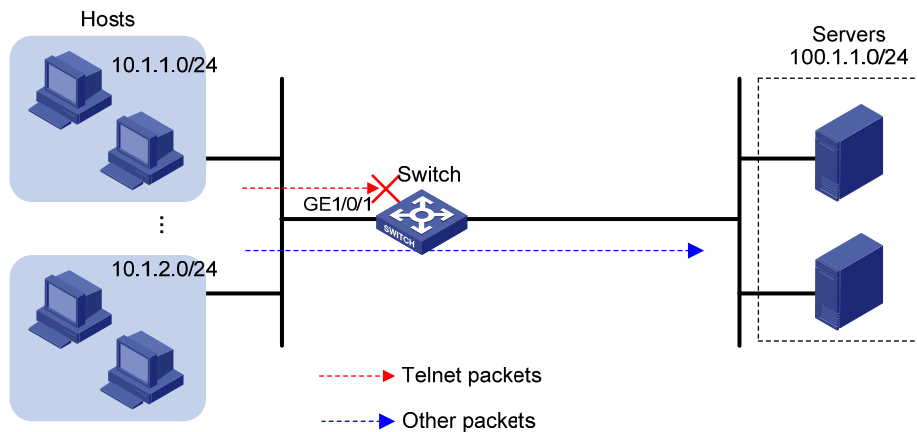
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 35](#), apply an ACL to GigabitEthernet 1/0/1 so that the interface drops all incoming Telnet packets and allows other IP packets to pass through.

Figure 35 Network diagram



Requirements analysis

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

Configuration restrictions and guidelines

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

Configuration procedures

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

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

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

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

Verifying the configuration

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

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

Out-bound Policy:

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

Ping a server on subnet 100.1.1.0/24 from a host. The server can be pinged successfully.

Use the host to Telnet the same server that supports Telnet services. The Telnet operation fails.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

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

Example: Allowing TCP connections initiated from a specific subnet

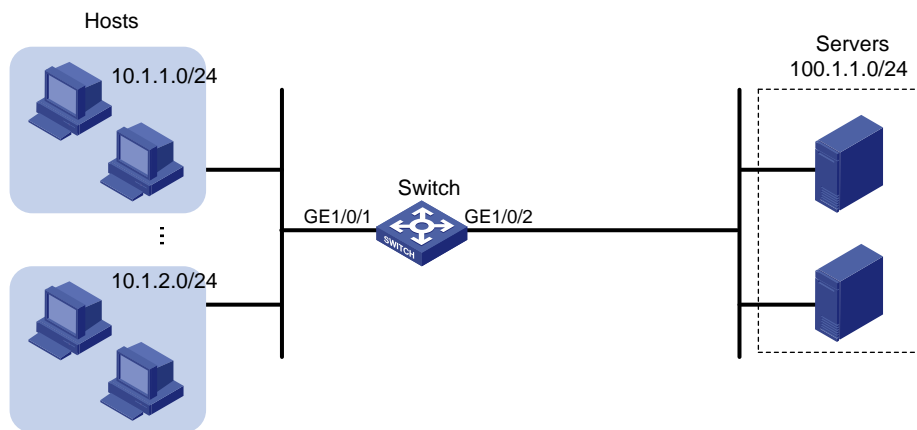
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 36](#), apply an ACL to allow TCP connections between the hosts and servers except the TCP connections initiated by the servers to hosts on subnet 10.1.1.0/24.

Figure 36 Network diagram



Requirements analysis

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

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

Configuration restrictions and guidelines

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

- 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 from the servers to the hosts on subnet 10.1.1.0/24.
- 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 connection 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 GigabitEthernet 1/0/2.

```
[Switch] interface gigabitEthernet 1/0/2
```

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

Verifying the configuration

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

```
[Switch] display packet-filter interface GigabitEthernet 1/0/2
```

```
Interface: GigabitEthernet1/0/2
```

```
  In-bound Policy:
```

```
    acl 3000, Successful
```

```
  Out-bound Policy:
```

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

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

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

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

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
```

```
acl number 3000
```

```
  rule 0 permit tcp established source 100.1.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 destination-port gt 1023
```

```
  rule 5 deny tcp source 100.1.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
```

```
#
```

```
interface GigabitEthernet1/0/2
```

```
  port link-mode bridge
```

```
  packet-filter 3000 inbound
```

```
#
```

Example: Denying FTP traffic

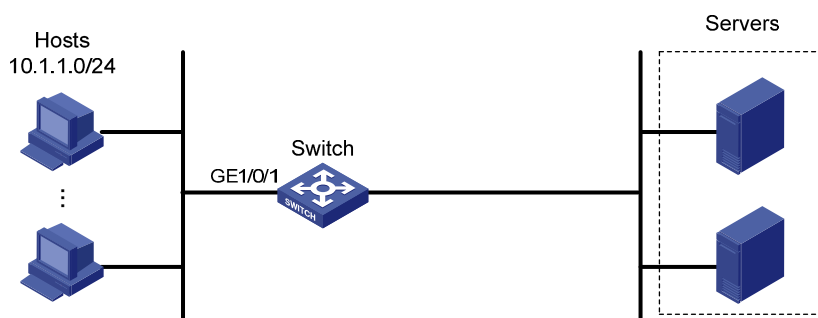
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in Figure 37, apply an ACL to GigabitEthernet 1/0/1 to deny FTP traffic destined for the servers.

Figure 37 Network diagram



Requirements analysis

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

Configuration restrictions and guidelines

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

Configuration procedures

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

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

```
[Switch-acl-adv-3000] rule deny tcp destination-port range 20 21
[Switch-acl-adv-3000] quit

# Apply ACL 3000 to filter incoming packets on GigabitEthernet 1/0/1.
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] packet-filter 3000 inbound
```

Verifying the configuration

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

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

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

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

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

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

Example: Allowing FTP traffic (active FTP)

This example provides an ACL application to allow FTP traffic when FTP operates in active mode. In this mode, the client initiates the control connection, and the server initiates the data connection from the server's port 20 to the client specified random port. If the client is behind the firewall, no connection can be established.

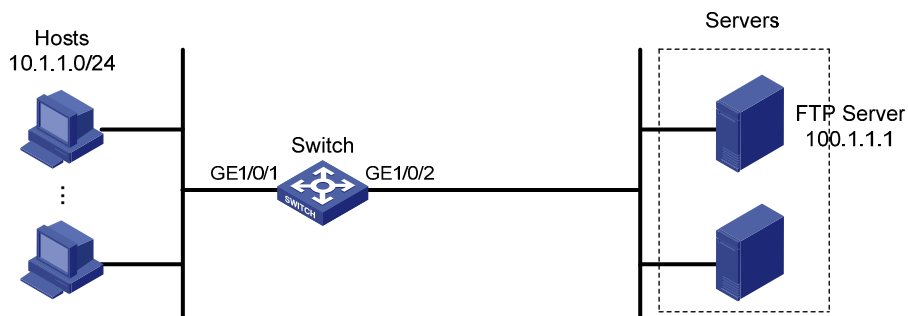
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 38](#), apply an ACL so that only active FTP traffic is allowed and all other IP traffic is denied.

Figure 38 Network diagram



Requirements analysis

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 GigabitEthernet 1/0/1.

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

Create IPv4 advanced ACL 3001.

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

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

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

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

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

Configure a rule to deny all IP packets.

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

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

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

Verifying the configuration

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

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

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

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

Verify that you can obtain data from a server through FTP when the server operates in active FTP mode.

Verify that you cannot obtain data from a server through FTP when the server operates in passive FTP mode.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

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

Example: Allowing FTP traffic (passive FTP)

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

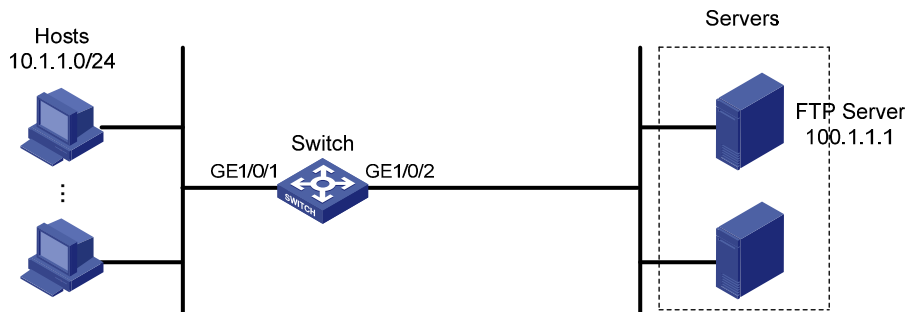
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 39](#), apply an ACL so that only passive FTP traffic is allowed and all other IP traffic is denied.

Figure 39 Network diagram



Requirements analysis

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 GigabitEthernet 1/0/1.

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

Create IPv4 advanced ACL 3001.

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

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

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

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

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

Configure a rule to deny all IP packets.

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

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

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

Verifying the configuration

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

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

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

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

Verify that you can obtain data from a server through FTP when the server operates in passive FTP mode.

Verify that you cannot obtain data from a server through FTP when the server operates in active FTP mode.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
acl number 3000
  rule 0 permit tcp destination 100.1.1.1 0 destination-port eq ftp
  rule 5 permit tcp destination 100.1.1.1 0 destination-port gt 1024
  rule 10 deny ip
acl number 3001
  rule 0 permit tcp source 100.1.1.1 0 source-port eq ftp established
  rule 5 permit tcp source 100.1.1.1 0 source-port gt 1024 established
  rule 10 deny ip
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  packet-filter 3000 inbound
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  packet-filter 3001 inbound
```

Example: Allowing ICMP requests from a specific direction

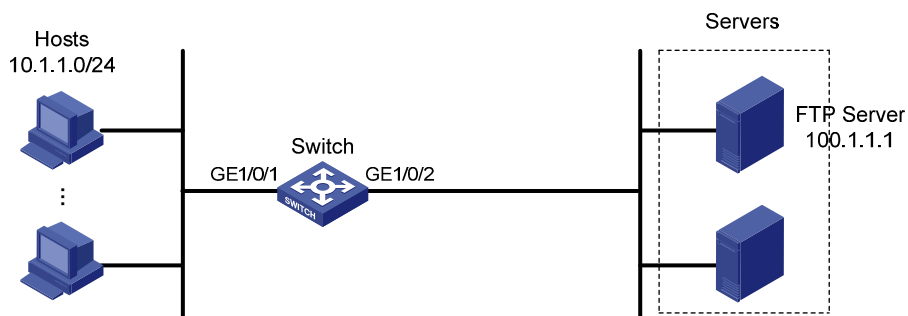
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 40](#), apply an ACL to deny ICMP requests from the FTP server to the hosts. Only hosts can ping the FTP server.

Figure 40 Network diagram



Requirements analysis

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

Configuration procedures

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

```
<Switch> system-view
[Switch] acl number 3000
[Switch-acl-adv-3000] rule deny icmp icmp-type echo
[Switch-acl-adv-3000] quit
```

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

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

Verifying the configuration

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

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

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

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

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

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

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

Example: Allowing HTTP/email/DNS traffic

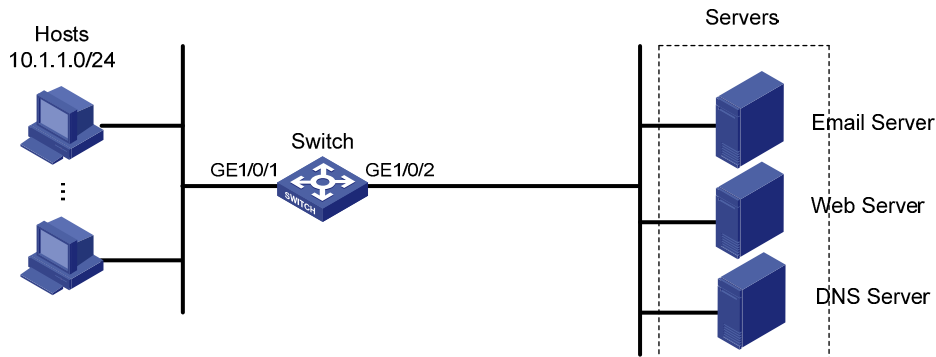
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 41](#), apply an ACL to GigabitEthernet 1/0/1 to allow only Email, HTTP, and DNS traffic from the server to the hosts. The rest of the traffic sourced from the servers to the hosts is denied.

Figure 41 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 GigabitEthernet 1/0/1.

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

Verifying the configuration

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

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

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

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

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.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

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

Example: Filtering packets by MAC address

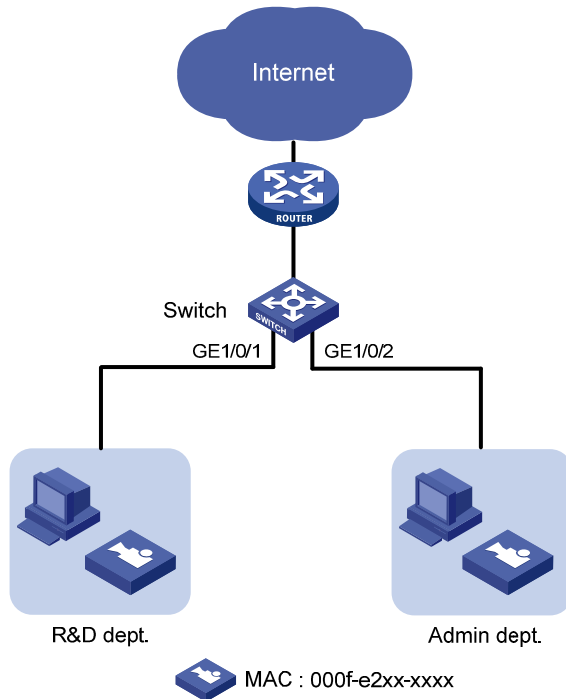
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in Figure 42, 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 42 Network diagram



Requirements analysis

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

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

Verifying the configuration

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

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

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

Verify that video devices can communicate with devices in the external network only during the working hours.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

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


Example: Applying ACLs in device management

Applicable product matrix

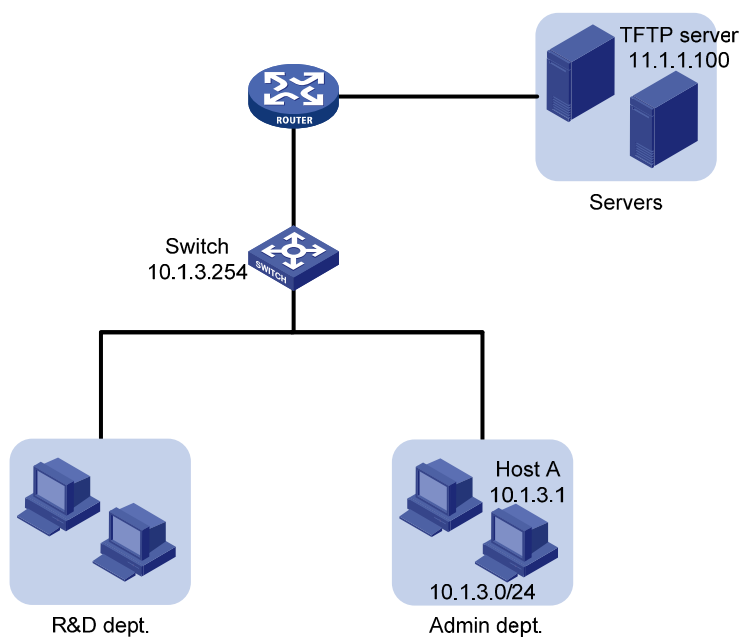
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 43](#), 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 43 Network diagram



Requirements analysis

To control access to Telnet, FTP, and TFTP, 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 all VTY user interfaces to allow only Host A to Telnet to the switch.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] acl 2000 inbound
```
- Control access to the TFTP server:
 - # Create IPv4 basic ACL 2001 and configure a rule to allow IP packets only sourced from the TFTP server.

```
[Switch] acl number 2001
[Switch-acl-basic-2001] rule permit source 11.1.1.100 0
[Switch-acl-basic-2001] quit
```
 - # Apply ACL 2001 to control the access to the TFTP server.

```
[Switch] tftp-server acl 2001
```
- Control access to the FTP server:
 - # Create IPv4 basic ACL 2002 and configure a rule to allow IP packets only sourced from Host A.

```
[Switch] acl number 2002
[Switch-acl-basic-2002] rule permit source 10.1.3.1 0
[Switch-acl-basic-2002] quit
```
 - # Enable FTP server on the switch.

```
[Switch] ftp server enable
```
 - # Apply ACL 2002 to allow only Host A to access the FTP server.

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

Verifying the configuration

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

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
ftp server enable
ftp server acl 2002
#
time-range telnet 08:30 to 18:00 working-day
#
acl number 2000
rule 0 permit source 10.1.3.1 0 time-range telnet
acl number 2001
rule 0 permit source 11.1.1.100 0
acl number 2002
rule 0 permit source 10.1.3.1 0
#
tftp-server acl 2001
#
user-interface vty 0 4
acl 2000 inbound
```

ARP attack protection configuration examples

This chapter provides ARP attack protection configuration examples.

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

Example: Configuring ARP source suppression and ARP blackhole routing

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

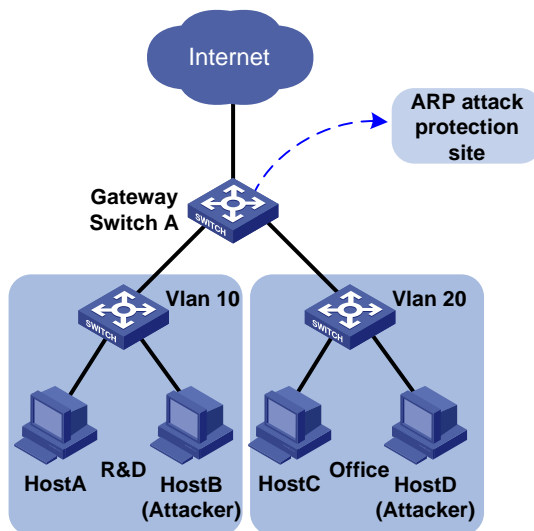
Network requirements

As shown in [Figure 44](#), Host B sends a large number of unresolvable IP packets with the same source address, and Host D sends a large number of unresolvable IP packets with different source addresses.

Configure ARP source suppression and ARP 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 44 Network diagram



Configuration procedures

1. Configuring ARP source suppression:

Enable ARP source suppression on Switch A.

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

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

```
[SwitchA] arp source-suppression limit 100
```

2. Enable ARP 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  
Current cache length: 16
```

Table 2 Command output

Field	Description
Current suppression limit	Maximum number of unresolvable IP packets that can be received from the same source address within 5 seconds.

Field	Description
Current cache length	Cache size for recording the ARP source suppression information.

Configuration files

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

Example: Configuring source MAC-based ARP attack detection

Applicable product matrix

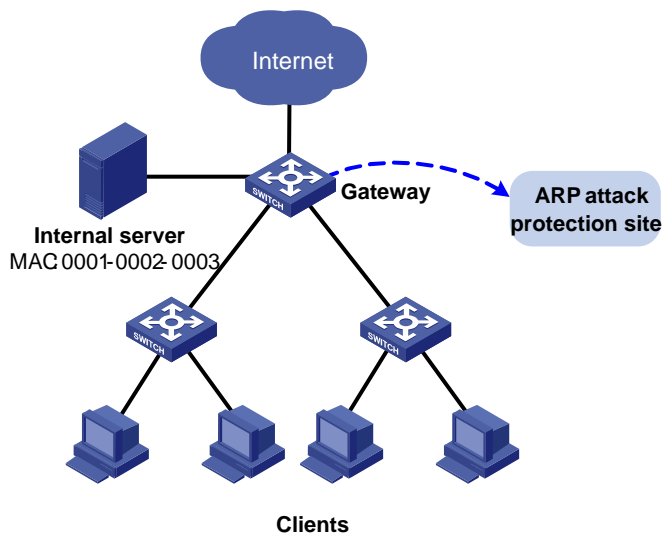
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 45](#), 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 45 Network diagram



Configuration procedures

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

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

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

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

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

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

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

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

Verifying the configuration

Display source MAC-based ARP attack detection entries.

```
<Sysname> display arp anti-attack source-mac slot 2
```

Source-MAC	VLAN ID	Interface	Aging-time
23f3-1122-3344	4094	GE2/0/1	10
23f3-1122-3355	4094	GE2/0/2	30
23f3-1122-33ff	4094	GE2/0/3	25
23f3-1122-33ad	4094	GE2/0/4	30
23f3-1122-33ce	4094	GE2/0/5	2

Configuration files

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

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

Applicable product matrix

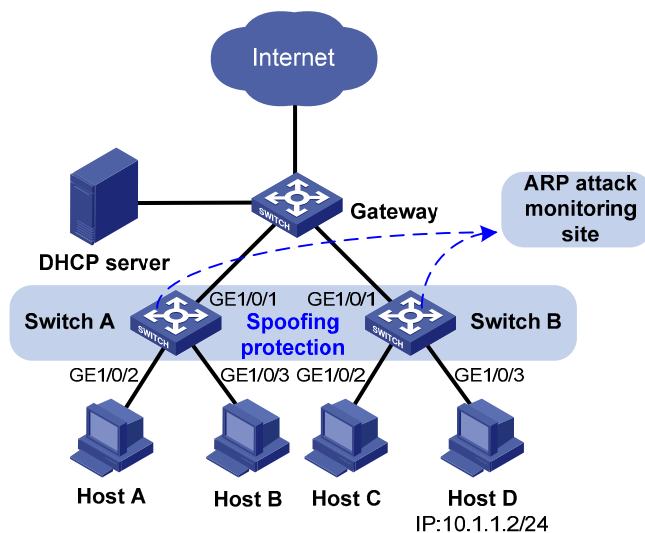
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 46](#), 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, and 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. The feature also discards the packets from Host D.

Figure 46 Network diagram



Requirements analysis

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

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

Configuration restrictions and guidelines

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

Configuration procedures

1. Configure Switch A:

Configure DHCP snooping.

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

Enable ARP detection for VLAN 1 for user validity check.

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

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

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

Enable ARP packet validity check.

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

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

Verifying the configuration

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

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

Configuration files

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

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

Applicable product matrix

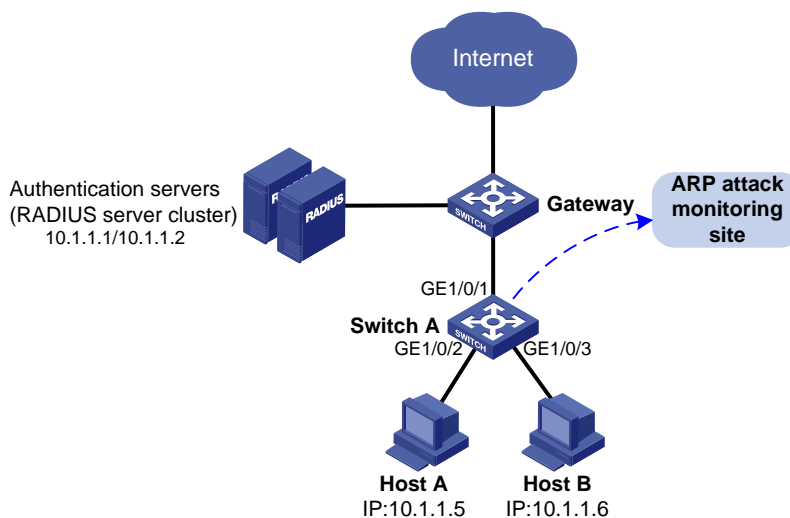
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 47](#), 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 47 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

Configure the local user account: add local user named **localuser**, set the password to **localpass** in plain text, and set the idle timeout period to 20 seconds.

```
<SwitchA> system-view
[SwitchA] local-user localuser
[SwitchA-luser-localuser] service-type lan-access
[SwitchA-luser-localuser] password simple localpass
[SwitchA-luser-localuser] authorization-attribute idle-cut 20
[SwitchA-luser-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 name
```

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

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

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

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

Set the real-time accounting interval to 15 minutes.

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

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

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

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

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

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

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

```

# Set a limit of 30 user connections for ISP domain aabbcc.net.
[SwitchA-isp-aabbcc.net] access-limit enable 30

# Specify the idle timeout period for the user as 20 seconds.
[SwitchA-isp-aabbcc.net] idle-cut enable 20
[SwitchA-isp-aabbcc.net] quit

# Configure aabbcc.net as the default ISP domain.
[SwitchA] domain default enable aabbcc.net

# Enable 802.1X on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.
[SwitchA] dot1x
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] dot1x
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] dot1x
[SwitchA-GigabitEthernet1/0/3] quit

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

```

Verifying the configuration

```

# Ping the gateway from Host A and Host B. Both ping operations are successful.

```

Configuration files

```

#
 domain default enable aabbcc.net
#
 dot1x
#
 vlan 1
  arp detection enable
#
 radius scheme radius1
  primary authentication 10.1.1.1
  primary accounting 10.1.1.2
  secondary authentication 10.1.1.2
  secondary accounting 10.1.1.1

```

```

key authentication cipher $c$3$DdOHTCT8yNBZxYvle7XkD2Ls5i+A8To=
key accounting cipher $c$3$2lMkqUQ+POWiHNKtd0a3fwYxlvWvuRp+
timer realtime-accounting 15
timer response-timeout 5
user-name-format without-domain
retry 5
#
domain aabbcc.net
authentication default radius-scheme radius1 local
authorization default radius-scheme radius1 local
accounting default radius-scheme radius1 local
access-limit enable 30
state active
idle-cut enable 20 10240
self-service-url disable
#
local-user localuser
password cipher $c$3$QF9jpm2ZxRQA8YS5+qedkwIPkWXuIc8FHb+qyQ==
authorization-attribute idle-cut 20
service-type lan-access
#
interface GigabitEthernet1/0/1
arp detection trust
#
interface GigabitEthernet1/0/2
dot1x
#
interface GigabitEthernet1/0/3
dot1x
#

```

ARP configuration examples

This chapter provides ARP configuration examples.

Example: Configuring ARP

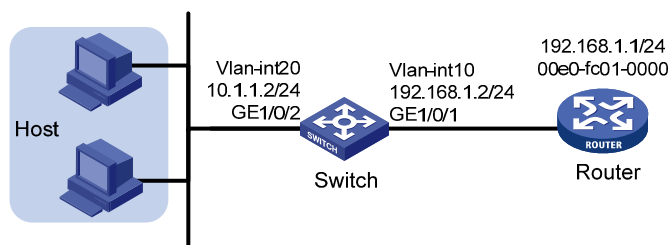
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 48](#), 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 48 Network diagram



Configuration procedures

Create VLAN 10.

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

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

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

Create VLAN-interface 10 and configure its IP address.

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

Create VLAN 20.

```

[Switch] vlan 20
[Switch-vlan20] quit

# Add interface GigabitEthernet 1/0/2 to VLAN 20.
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] port access vlan 20
[Switch-GigabitEthernet1/0/2] quit

# Create VLAN-interface 20 and configure its IP address.
[Switch] interface vlan-interface 20
[Switch-vlan-interface20] ip address 10.1.1.2 24
[Switch-vlan-interface20] quit

# Set the aging timer for dynamic ARP entries to 5 minutes.
[Switch] arp timer aging 5

# Configure a static ARP entry that has IP address 192.168.1.1, MAC address 00e0-fc01-0000, and
output interface GigabitEthernet 1/0/1 in VLAN 10.
[Switch] arp static 192.168.1.1 00e0-fc01-0000 10 GigabitEthernet 1/0/1

```

Verifying the configuration

Display all ARP entries on the switch.

```

<Switch> display arp

```

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

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```

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

```



```
port access vlan 20
#
arp timer aging 5
arp static 192.168.1.1 00e0-fc01-0000 10 GigabitEthernet1/0/1
#
```

Proxy ARP configuration examples

This chapter provides proxy ARP configuration examples.

Proxy ARP enables hosts on different broadcast domains to communicate with each other as 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

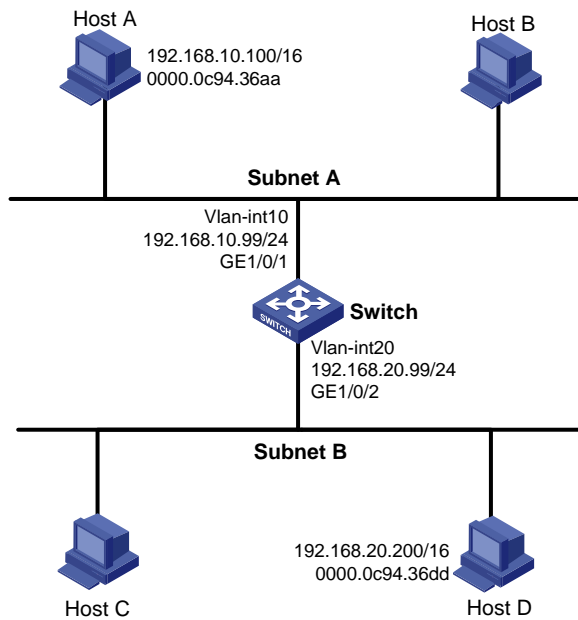
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 49](#), configure common proxy ARP on the switch to enable communication between Host A and Host D.

Figure 49 Network diagram



Configuration procedures

Create VLAN 10.

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

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

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

Create VLAN-interface 10 and configure its IP address.

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

Create VLAN 20.

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

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

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

Create VLAN-interface 20 and configure its IP address.

```
[Switch] interface vlan-interface 20
```

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

# Enable common proxy ARP on interface VLAN-interface 10.
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] proxy-arp enable
[Switch-Vlan-interface10] quit

# Enable common proxy ARP on interface VLAN-interface 20.
[Switch] interface vlan-interface 20
[Switch-Vlan-interface20] proxy-arp enable
```

Verifying the configuration

```
# Display the common proxy ARP status on the switch.
<Switch> display proxy-arp
Interface Vlan-interface10
  Proxy ARP status: enabled

Interface Vlan-interface20
  Proxy ARP status: enabled

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

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

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

Example: Configuring local proxy ARP

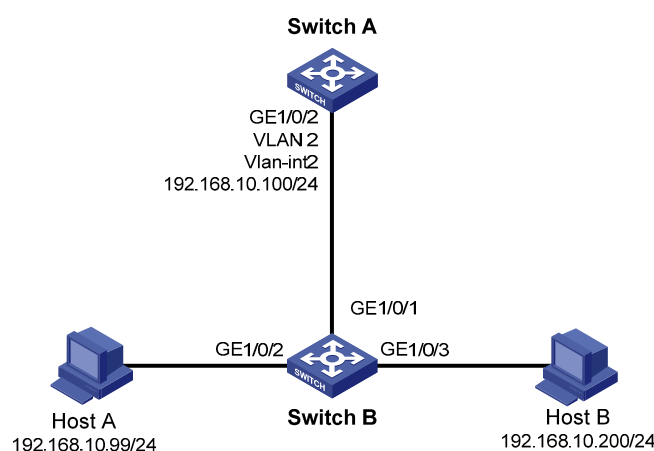
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 50](#), 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 50 Network diagram



Configuration procedures

1. Configure Switch A:

Configure the IP address of interface VLAN-interface 2.

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

Enable local proxy ARP on interface VLAN-interface 2.

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

2. Configure Switch B:

```

# Add interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 2.
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1
[SwitchB-vlan2] port gigabitethernet 1/0/2
[SwitchB-vlan2] port gigabitethernet 1/0/3
[SwitchB-vlan2] quit

# Configure port isolation on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port-isolate enable
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port-isolate enable
[SwitchB-GigabitEthernet1/0/3] quit

```

Verifying the configuration

Display local proxy ARP status on Switch A.

```

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

```

Display port isolation information on Switch B.

```

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

```

Ping Host B from Host A. The ping operation is successful. 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

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:


```

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

```

```
port link-mode bridge
port access vlan 2
#
```

- Switch B:

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

BPDU tunneling configuration examples

This chapter provides BPDU tunneling configuration examples.

Example: Configuring BPDU tunneling for STP

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

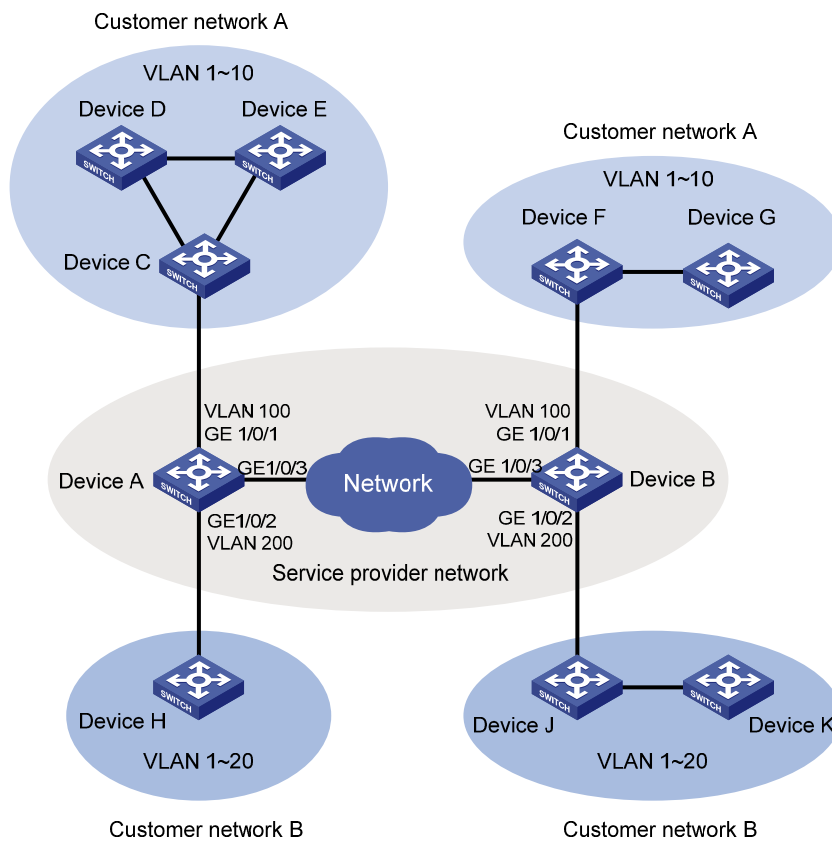
As shown in [Figure 51](#):

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

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

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

Figure 51 Network diagram



Configuration restrictions and guidelines

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

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

Configuration procedures

Configure Device A

1. Configure GigabitEthernet 1/0/1:
Assign port GigabitEthernet 1/0/1 to VLAN 100.

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

```
[DeviceA-GigabitEthernet1/0/1] port access vlan 100
# Enable basic QinQ on the port.
[DeviceA-GigabitEthernet1/0/1] qinq enable
# Disable STP on the port GigabitEthernet 1/0/1.
[DeviceA-GigabitEthernet1/0/1] undo stp enable
# Enable BPDU tunneling for STP on the port.
[DeviceA-GigabitEthernet1/0/1] bpdu-tunnel dot1q stp
[DeviceA-GigabitEthernet1/0/1] quit
```

2. Configure GigabitEthernet 1/0/2:

```
# Assign port GigabitEthernet 1/0/2 to VLAN 200.
[DeviceA] vlan 200
[DeviceA-vlan200] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port access vlan 200
# Enable basic QinQ on the port.
[DeviceA-GigabitEthernet1/0/2] qinq enable
# Disable STP on the port GigabitEthernet 1/0/2.
[DeviceA-GigabitEthernet1/0/2] undo stp enable
# Enable BPDU tunneling for STP on the port.
[DeviceA-GigabitEthernet1/0/2] bpdu-tunnel dot1q stp
[DeviceA-GigabitEthernet1/0/2] quit
```

3. Configure GigabitEthernet 1/0/3:

```
# Configure the network-side port GigabitEthernet 1/0/3 as a trunk port.
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
# Assign GigabitEthernet 1/0/3 to VLANs 100 and 200.
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 100 200
# Remove GigabitEthernet 1/0/3 from VLAN 1.
[DeviceA-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/3] quit
```

Configuring DeviceB

1. Configure GigabitEthernet 1/0/1:

```
# Assign port GigabitEthernet 1/0/1 to VLAN 100.
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] quit
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port access vlan 100
# Enable basic QinQ on the port.
[DeviceB-GigabitEthernet1/0/1] qinq enable
# Disable STP on the port GigabitEthernet 1/0/1.
```

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
# Enable BPDU tunneling for STP on the port.
[DeviceB-GigabitEthernet1/0/1] bpdu-tunnel dot1q stp
[DeviceB-GigabitEthernet1/0/1] quit
```

2. Configure GigabitEthernet 1/0/2:

```
# Assign port GigabitEthernet 1/0/2 to VLAN 200.
[DeviceB] vlan 200
[DeviceB-vlan200] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port access vlan 200
# Enable basic QinQ on the port.
[[DeviceB-GigabitEthernet1/0/2] qinq enable
# Disable STP on the port GigabitEthernet 1/0/2.
[DeviceB-GigabitEthernet1/0/2] undo stp enable
# Enable BPDU tunneling for STP on the port.
[DeviceB-GigabitEthernet1/0/2] bpdu-tunnel dot1q stp
[DeviceB-GigabitEthernet1/0/2] quit
```

3. Configure GigabitEthernet 1/0/3:

```
# Configure the network-side port GigabitEthernet 1/0/3 as a trunk port.
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
# Assign GigabitEthernet 1/0/3 to VLANs 100 and 200.
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 100 200
# Remove GigabitEthernet 1/0/3 from VLAN 1.
[DeviceB-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/3] quit
```

Verifying the configuration

Execute the **display stp bpdu-statistics interface** *interface-type interface-number* command on Device C and Device F to display the following statistics:

- The BPDU statistics of the port connecting Device C to Device A.
- The BPDU statistics of the port connecting Device F to Device B.

The BPDU statistics show that the two ports can receive STP BPDUs from the peer ends.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- DeviceA:
#

```

vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
 stp disable
 bpdu-tunnel dot1q stp
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
 stp disable
 bpdu-tunnel dot1q stp
 qinq enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#

```

- DeviceB:

```

#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
 stp disable
 bpdu-tunnel dot1q stp
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
 stp disable
 bpdu-tunnel dot1q stp
 qinq enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1

```

```
port trunk permit vlan 100 200
#
```

CFD configuration examples

This chapter provides Connectivity Fault Detection (CFD) configuration examples.

Use CFD in Layer 2 networks to implement link connectivity detection, fault verification, and fault location.

General configuration restrictions and guidelines

Devices in the same MD must use the same CFD protocol version. Otherwise, they cannot exchange CFD protocol packets.

Example: Configuring CFD

Applicable product matrix

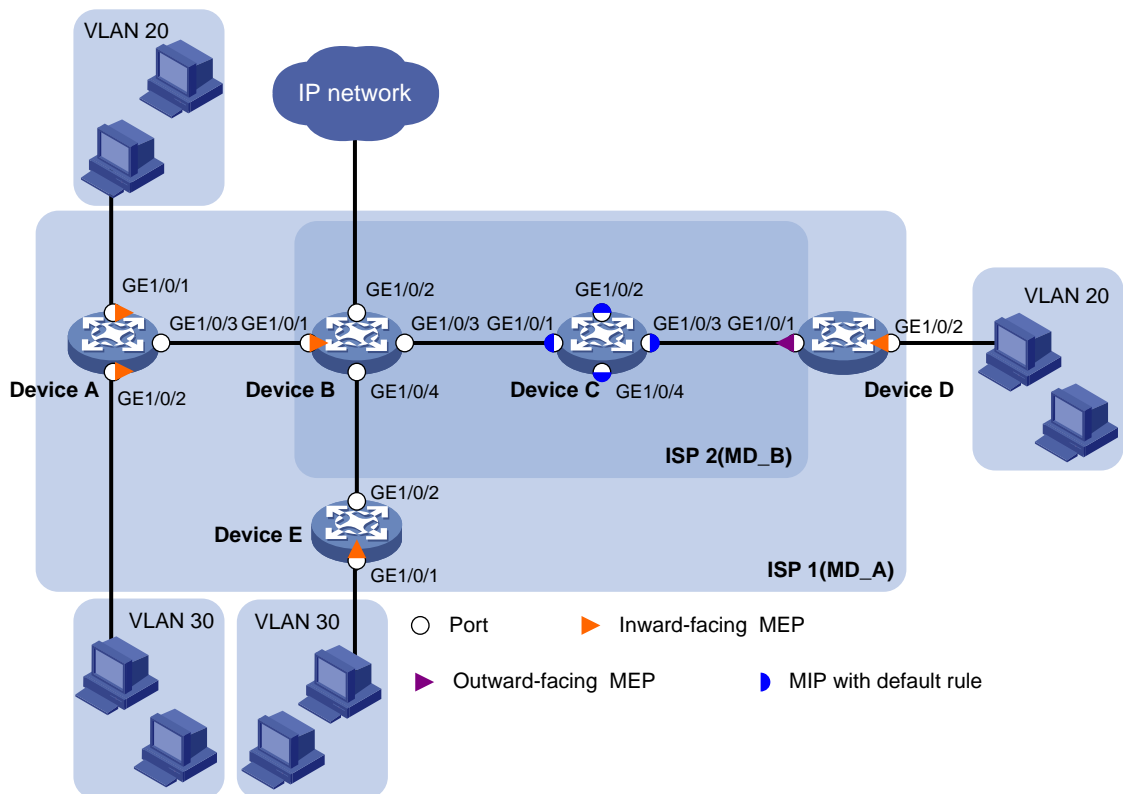
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 52](#), 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 52 Network diagram



Requirements analysis

To effectively implement CFD, assign devices of an ISP to the same MD, and 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

On the devices as shown in [Figure 52](#), create VLANs 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 MA_A_1, which serves VLAN 20, in MD_A.

```
[DeviceA] cfd ma MA_A_1 md MD_A vlan 20
```

Create service instance 1 for MD_A and MA_A_1.

```
[DeviceA] cfd service-instance 1 md MD_A ma MA_A_1
```

Create MA_A_2, which serves VLAN 30, in MD_A.

```
[DeviceA] cfd ma MA_A_2 md MD_A vlan 30
```

Create service instance 2 for MD_A and MA_A_2.

```
[DeviceA] cfd service-instance 2 md MD_A ma MA_A_2
```

Configure Device B through Device E in the same way Device A is configured.

2. Configure Device B:

```
[DeviceB] cfd md MD_B level 3
```

```
[DeviceB] cfd ma MA_B_1 md MD_B vlan 20
```

```
[DeviceB] cfd service-instance 3 md MD_B ma MA_B_1
```

3. Configure Device C:

```
[DeviceC] cfd md MD_B level 3
```

```
[DeviceC] cfd ma MA_B_1 md MD_B vlan 20
```



```
[DeviceC] cfd service-instance 3 md MD_B ma MA_B_1
```

4. Configure Device D:

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

5. Configure Device E:

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

Configuring MEPs

Assign MEP IDs as described in the following table:

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

1. Configure Device A:

Configure a MEP list in service instances 1 and 2.

```
[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] cfd meplist 2001 2002 service-instance 2
```

Create and enable inward-facing MEP 1001 in service instance 1 on GigabitEthernet 1/0/1.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 inbound
[DeviceA-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

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

```
[DeviceA] interface GigabitEthernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 inbound
[DeviceA-GigabitEthernet1/0/2] cfd mep service-instance 2 mep 2001 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Configure Device B, Device D, and Device E in the same way Device A is configured.

2. Configure Device B:

```
[DeviceB] cfd meplist 3001 3002 service-instance 3
[DeviceB] interface GigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] cfd mep 3001 service-instance 3 inbound
```

```
[DeviceB-GigabitEthernet1/0/1] cfd mep service-instance 3 mep 3001 enable
[DeviceB-GigabitEthernet1/0/1] quit
```

3. Configure Device D:

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

4. Configure Device E:

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

Configuring a MIP generation rule

MIP configuration is optional. MIPs process LTM frames and LBM frames, and they can help you 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 GigabitEthernet 1/0/1.

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

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

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

Configure Device B, Device D, and Device E in the same way Device A is configured.

2. Configure Device B:

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

3. Configure Device D:

```
[DeviceD] interface GigabitEthernet 1/0/1
```

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

4. Configure Device E:

```
[DeviceE] interface GigabitEthernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] cfd cc service-instance 2 mep 2002 enable
[DeviceE-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display information about remote MEP 1001 in service instance 1 on Device A.

```
[DeviceA] display cfd remote-mep service-instance 1 mep 1001
MEP ID      MAC Address      State      Time                      MAC Status
1002       0010-FC00-6514   OK         2013/02/01 12:54:52     UP
```

The remote MEP is operating correctly.

Enable LB on Device A to check the status of the link between MEP 1001 and MEP 1002 in service instance 1.

```
[DeviceA] cfd loopback service-instance 1 mep 1001 target-mep 1002
Loopback to 0010-FC00-6514 with the sequence number start from 1001-43404:
Reply from 0010-FC00-6514: sequence number=1001-43404
Reply from 0010-FC00-6514: sequence number=1001-43405
Reply from 0010-FC00-6514: sequence number=1001-43406
Reply from 0010-FC00-6514: sequence number=1001-43407
Reply from 0010-FC00-6514: sequence number=1001-43408
Send:5          Received:5      Lost:0
```

The output shows that no link fault occurs on the link between MEP 1001 and MEP 1002 in service instance 1.

Identify the path between MEP 3001 and MEP 3002 in service instance 3 on Device B.

```
[DeviceB] cfd linktrace service-instance 3 mep 3001 target-mep 3002
Linktrace to MEP 3002 with the sequence number 3001-34
MAC Address      TTL      Last MAC      Relay Action
0010-FC00-6513   63       0010-FC00-6512  FDB
0010-FC00-6514   62       0010-FC00-6513  Hit
```

The output shows that MEP 3001 locates MEP 3002 in service instance 3. After receiving LTM messages from the source MEP, MIPs on the path and the target MEP send LTR messages to the source MEP. The source MEP then identifies the path between MEP 3001 and MEP 3002.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```

#
 cfd enable
 cfd md MD_A level 5
 cfd ma MA_A_1 md MD_A vlan 20
 cfd service-instance 1 md MD_A ma MA_A_1
 cfd meplist 1001 to 1002 service-instance 1
 cfd ma MA_A_2 md MD_A vlan 30
 cfd service-instance 2 md MD_A ma MA_A_2
 cfd meplist 2001 to 2002 service-instance 2
#
vlan 20
#
vlan 30
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 20
 cfd mep 1001 service-instance 1 inbound
 cfd mep service-instance 1 mep 1001 enable
 cfd cc service-instance 1 mep 1001 enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 30
 cfd mep 2001 service-instance 2 inbound
 cfd mep service-instance 2 mep 2001 enable
 cfd cc service-instance 2 mep 2001 enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 20 30

```

- **Device B:**

```

#
 cfd enable
 cfd md MD_B level 3
 cfd ma MA_B_1 md MD_B vlan 20
 cfd service-instance 3 md MD_B ma MA_B_1
 cfd meplist 3001 to 3002 service-instance 3
#
vlan 20
#
vlan 30
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 20 30

```

```

cfd mep 3001 service-instance 3 inbound
cfd mep service-instance 3 mep 3001 enable
cfd cc service-instance 3 mep 3001 enable
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 20 30
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
port trunk permit vlan 20
#
interface GigabitEthernet1/0/4
port link-mode bridge
port link-type trunk
port trunk permit vlan 30

```

- Device C:

```

#
cfd enable
cfd md MD_B level 3
cfd ma MA_B_1 md MD_B vlan 20
cfd service-instance 3 md MD_B ma MA_B_1
cfd mip-rule default service-instance 3
#
vlan 20
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 20
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 20
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
port trunk permit vlan 20
#
interface GigabitEthernet1/0/4
port link-mode bridge
port link-type trunk
port trunk permit vlan 30

```

- Device D:

```

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

```

- Device E:

```

#
 cfd enable
 cfd md MD_A level 5
 cfd ma MA_A_2 md MD_A vlan 30
 cfd service-instance 2 md MD_A ma MA_A_2
 cfd meplist 2001 to 2002 service-instance 2
#
vlan 30
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 30
 cfd mep 2002 service-instance 2 inbound
 cfd mep service-instance 2 mep 2002 enable
 cfd cc service-instance 2 mep 2002 enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 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

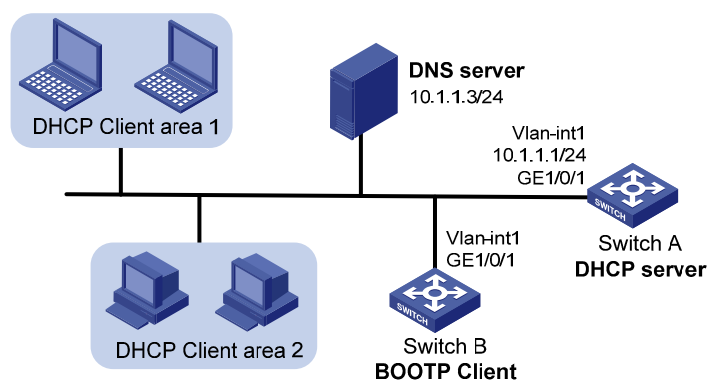
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 53](#), configure the DHCP server on Switch A to implement the following:

- Dynamically assign IP addresses, lease duration, DNS information, and gateway addresses to DHCP clients on subnet 10.1.1.0/24.
- Assign IP address, DNS information, and gateway address to Switch B according to the MAC address of Switch B.
- Detect unauthorized DHCP servers on the network.

Figure 53 Network diagram



Requirements analysis

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

- To make sure the IP address of the DNS server is not assigned to any client by the DHCP server, you must exclude it from dynamic address allocation.
- To enable administrators to locate unauthorized DHCP servers, you must enable the unauthorized DHCP server detection on the DHCP server. The server then records the IP address of all DHCP servers that assign IP addresses to clients and the interfaces receiving DHCP message.

Configuration restrictions and guidelines

To ensure correct address allocation, keep the IP addresses used for dynamic allocation on the subnet where the interface of the DHCP server resides if possible.

Configuration procedures

```
# Specify an IP address for VLAN-interface 1.
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.1.1.1 24

# Enable DHCP.
[SwitchA] dhcp enable

# Enable DHCP server on VLAN-interface 1.
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] dhcp select server global-pool
[SwitchA-Vlan-interface1] quit

# Exclude the IP address of the DNS server from address allocation.
[SwitchA] dhcp server forbidden-ip 10.1.1.3

# Configure DHCP address pool 0.
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] static-bind mac-address 000f-e249-8050
[SwitchA-dhcp-pool-0] static-bind ip-address 10.1.1.6 24
[SwitchA-dhcp-pool-0] dns-list 10.1.1.3
[SwitchA-dhcp-pool-0] domain-name com
[SwitchA-dhcp-pool-0] gateway-list 10.1.1.1
[SwitchA-dhcp-pool-0] quit

# Configure DHCP address pool 1.
[SwitchA] dhcp server ip-pool 1
[SwitchA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-1] dns-list 10.1.1.3
[SwitchA-dhcp-pool-1] domain-name com
[SwitchA-dhcp-pool-1] expired day 10
[SwitchA-dhcp-pool-1] gateway-list 10.1.1.1
[SwitchA-dhcp-pool-1] quit

# Enable unauthorized DHCP server detection.
```



```
[SwitchA] dhcp server detect
```

Verifying the configuration

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

Use the **display** commands to verify the DHCP information. For example, use the **display dhcp server tree** command to display DHCP address pool information.

```
[SwitchA] display dhcp server tree all
Global pool:
```

```
Pool name: 0
static-bind ip-address 10.1.1.6 mask 255.255.255.0
static-bind mac-address 000f-e249-8050
Parent node:1
gateway-list 10.1.1.1
dns-list 10.1.1.3
domain-name com
expired unlimited
```

```
Pool name: 1
network 10.1.1.0 mask 255.255.255.0
Child node:0
gateway-list 10.1.1.1
dns-list 10.1.1.3
domain-name com
expired 10 0 0 0
```

Use the **dhcp server ip-in-use** command to display IP-to-MAC binding information.

```
[SwitchA] display dhcp server ip-in-use all
Pool utilization: 1.18%
```

IP address	Client-identifier/ Hardware address	Lease expiration	Type
10.1.1.6	000f-e249-8050	NOT Used	Manual
10.1.1.2	3822-d63a-e106	May 3 2013 09:53:48	Auto:COMMITTED
10.1.1.4	3363-6535-2e61-3664- 662e-6531-3339-2d56- 6c61-6e2d-696e-7465- 7266-6163-6531	May 3 2013 09:54:10	Auto:COMMITTED

```
--- total 3 entry ---
```

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
vlan 1
```

```

#
dhcp server ip-pool 0
  static-bind ip-address 10.1.1.6 mask 255.255.255.0
  static-bind mac-address 000f-e249-8050
  gateway-list 10.1.1.1
  dns-list 10.1.1.3
  domain-name com
#
dhcp server ip-pool 1
  network 10.1.1.0 mask 255.255.255.0
  gateway-list 10.1.1.1
  dns-list 10.1.1.3
  domain-name com
  expired day 10
#
interface Vlan-interface1
  ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-mode bridge
#
dhcp server forbidden-ip 10.1.1.3
dhcp server detect
#
dhcp enable
#

```

Example: Configuring the DHCP relay agent

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 54](#), Switch A and Switch B can reach each other.

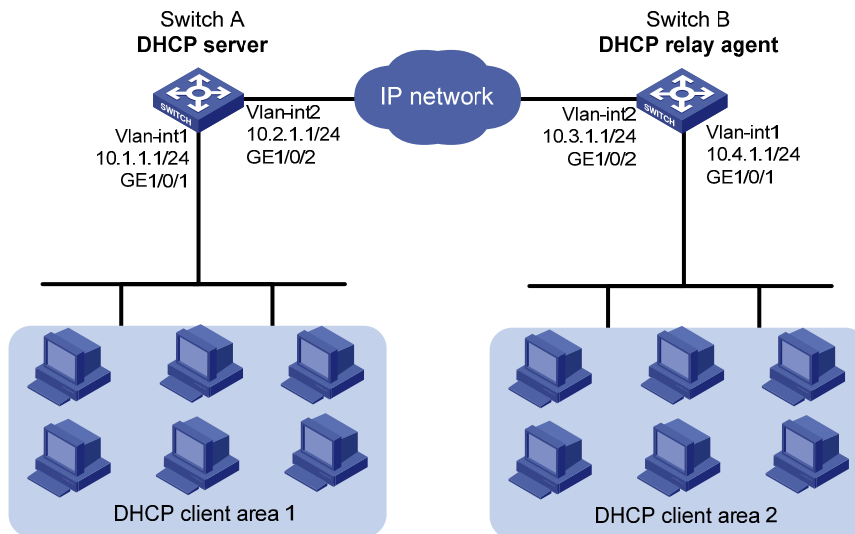
Configure the DHCP server on Switch A to assign IP addresses to clients in area 1.

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 54 Network diagram



Requirements analysis

To prevent hosts from using manually configured IP addresses to access the external network, you must enable address check on the DHCP relay agent.

Configuration restrictions and guidelines

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

- 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 IP address of the DHCP server must not reside on the same subnet as the IP address of the relay agent interface. Otherwise, the clients might fail to obtain IP addresses.
- Before enabling address check on an interface, enable the DHCP service and enable the DHCP relay agent on the interface. Otherwise, the address check configuration does not take effect.

Configuration procedures

Configuring Switch A

Specify IP addresses for VLAN interfaces.

```
<SwitchA> system-view
```

```

[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.1.1.1 24
[SwitchA-Vlan-interface1] quit
[SwitchA] vlan 2
[SwitchA-vlan2] port GigabitEthernet 1/0/2
[SwitchA-vlan2] quit
[SwitchA] interface Vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.2.1.1 24
[SwitchA-Vlan-interface2] quit

# Enable DHCP.
[SwitchA] dhcp enable

# Configure DHCP address pool 0.
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-0] quit

# Configure DHCP address pool 1.
[SwitchA] dhcp server ip-pool 1
[SwitchA-dhcp-pool-1] network 10.4.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-1] quit

```

Configuring Switch B

```

# Specify IP addresses for VLAN interfaces.
<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.4.1.1 24
[SwitchB-Vlan-interface1] quit
[SwitchB] vlan 2
[SwitchB-vlan2] port GigabitEthernet 1/0/2
[SwitchB-vlan2] quit
[SwitchB] interface Vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.3.1.1 24
[SwitchB-Vlan-interface2] quit

# Enable DHCP.
[SwitchB] dhcp enable

# Specify DHCP server 10.2.1.1 for DHCP server group 1 on the relay agent.
[SwitchB] dhcp relay server-group 1 ip 10.2.1.1

# Enable the DHCP relay agent on VLAN-interface 1.
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] dhcp select relay

# Apply DHCP server group 1 to VLAN-interface 1.
[SwitchB-Vlan-interface1] dhcp relay server-select 1

# Enable address check on the relay agent.
[SwitchB-Vlan-interface1] dhcp relay address-check enable

```

Verifying the configuration

Verify that the clients in area 1 and area 2 can obtain IP addresses and other configuration parameters from Switch A.

Use the **display** commands to verify the DHCP relay agent information on Switch B. For example, use the **display dhcp relay all** command to display DHCP server groups.

```
[SwitchB] display dhcp relay all
      Interface name                Server-group
      Vlan-interface1              1
```

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```
#
vlan 1
#
vlan 2
#
dhcp server ip-pool 0
  network 10.1.1.0 mask 255.255.255.0
#
dhcp server ip-pool 1
  network 10.4.1.0 mask 255.255.255.0
#
interface Vlan-interface1
  ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface2
  ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-mode bridge
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 2
#
dhcp enable
#
```

- Switch B:

```
#
dhcp relay server-group 1 ip 10.2.1.1
#
```

```
vlan 1
#
vlan 2
#
interface Vlan-interface1
 ip address 10.4.1.1 255.255.255.0
 dhcp select relay
 dhcp relay address-check enable
 dhcp relay server-select 1
#
interface Vlan-interface2
 ip address 10.3.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
dhcp enable

#
```

Example: Configuring DHCP relay agent support for Option 82

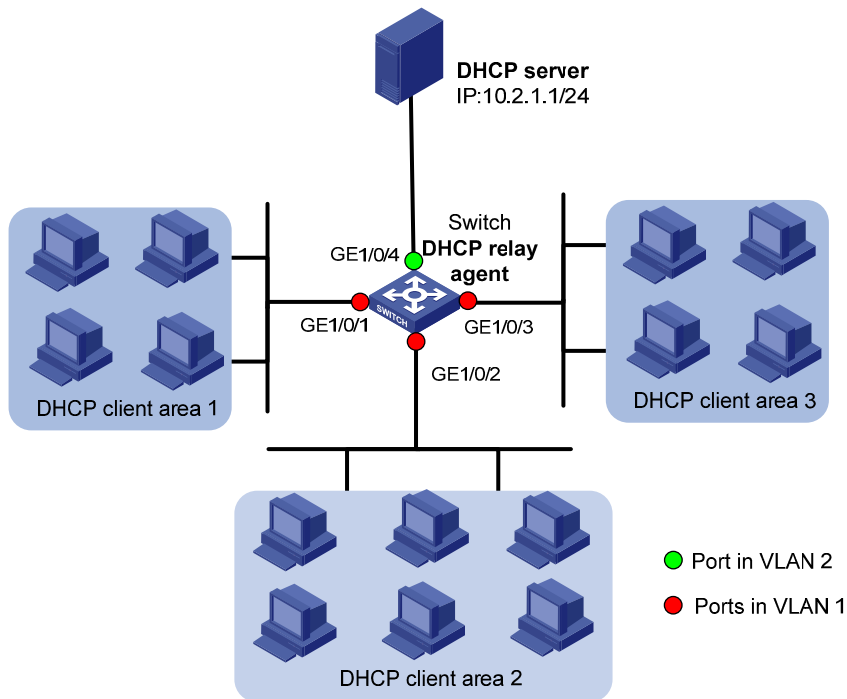
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 55](#), Option 82 configuration is completed on the DHCP server. Configure the DHCP relay agent to support Option 82 so the DHCP server can assign IP addresses in specific ranges to DHCP clients in different areas.

Figure 55 Network diagram



Configuration procedures

Specify IP addresses for VLAN interfaces.

```
<Switch> system-view
[Switch] interface Vlan-interface 1
[Switch-Vlan-interface1] ip address 10.1.1.1 24
[Switch-Vlan-interface1] quit
[Switch] vlan 2
[Switch-vlan2] port GigabitEthernet 1/0/4
[Switch-vlan2] quit
[Switch] interface Vlan-interface 2
[Switch-Vlan-interface2] ip address 10.2.1.2 24
[Switch-Vlan-interface2] quit
```

Enable DHCP.

```
[Switch] dhcp enable
```

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

```
[Switch] dhcp relay server-group 1 ip 10.2.1.1
```

Enable the DHCP relay agent on VLAN-interface 1.

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

Apply DHCP server group 1 to VLAN-interface 1.

```
[Switch-Vlan-interface1] dhcp relay server-select 1
```

```
# Enable the DHCP relay agent to support Option 82.
[Switch-Vlan-interface1] dhcp relay information enable
```

Verifying the configuration

Verify that DHCP clients can obtain IP addresses on specific subnets from the DHCP server.

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

```
[Switch] display dhcp relay information all
Interface: Vlan-interface1
    Status: Enable
    Strategy: Replace
    Format: Normal
```

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
dhcp relay server-group 1 ip 10.2.1.1
#
vlan 1
#
vlan 2
#
interface Vlan-interface1
ip address 10.1.1.1 255.255.255.0
dhcp select relay
dhcp relay server-select 1
dhcp relay information enable
#
interface Vlan-interface2
ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode bridge
#
interface GigabitEthernet1/0/2
port link-mode bridge
#
interface GigabitEthernet1/0/3
port link-mode bridge
#
interface GigabitEthernet1/0/4
port link-mode bridge
port access vlan 2
```



```
#
dhcp enable
#
```

Example: configuring DHCP snooping

Applicable product matrix

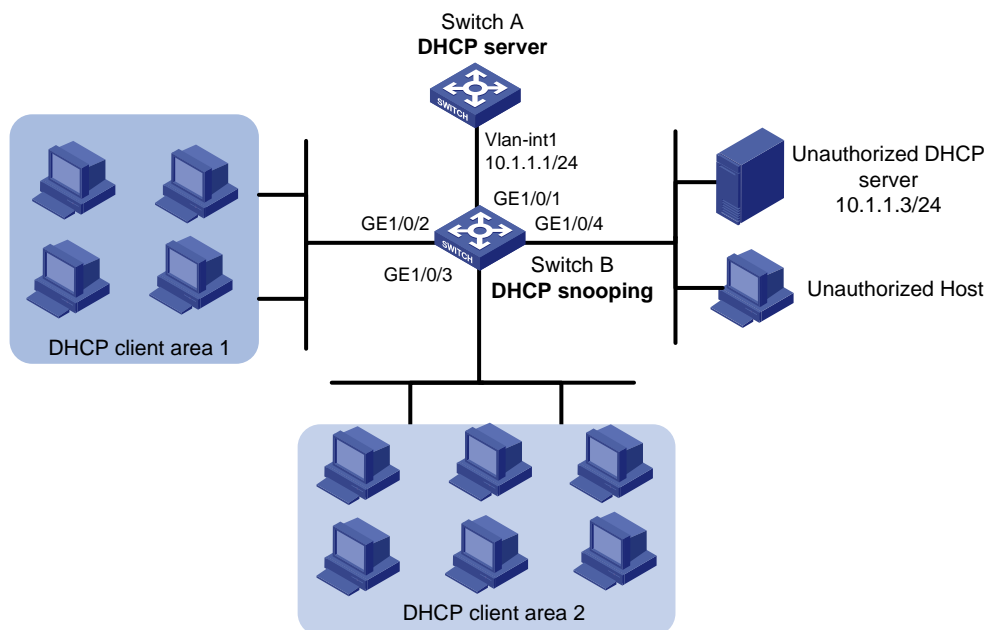
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 56](#), configure DHCP snooping on Switch B to implement the following:

- Make sure DHCP clients obtain IP addresses from the authorized DHCP server (Switch A).
- Prevent users from accessing the network through static IP addresses.

Figure 56 Network diagram



Requirements analysis

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

- To make sure Switch B forward DHCP messages from the authorized DHCP server to DHCP clients, you must configure GigabitEthernet 1/0/1 as trusted and configure other ports as untrusted.
- To prevent users from accessing the network through static IP addresses, you must enable ARP detection in VLAN 1 for user validity check.

Configuration procedures

Configuring Switch A

```
# Specify an IP address for VLAN-interface 1.
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.1.1.1 24

# Enable DHCP.
[SwitchA] dhcp enable

# Configure DHCP address pool 0.
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-1] quit
```

Configuring Switch B

```
# Enable DHCP snooping.
<SwitchB> system-view
[SwitchB] dhcp-snooping

# Specify GigabitEthernet 1/0/1 as a trusted port.
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] dhcp-snooping trust
[SwitchB-GigabitEthernet1/0/1] quit

# Enable ARP detection for user validity check.
[SwitchB] vlan 1
[SwitchB-vlan1] arp detection enable

# Specify GigabitEthernet 1/0/1 as an ARP trusted port. By default, a port is an ARP untrusted port.
[SwitchB-vlan1] quit
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] arp detection trust
[SwitchB-GigabitEthernet1/0/1] quit
```

Verifying the configuration

```
# Display DHCP snooping entries.
[SwitchB] display dhcp-snooping
DHCP Snooping is enabled.
The client binding table for all ports.
```

```

Type : D--Dynamic , S--Static , R--Recovering
Type IP Address      MAC Address      Lease      VLAN SVLAN Interface
=====
D    10.1.1.15       00e0-fc00-0006  286        1    N/A   GigabitEthernet1/0/1
---  1 dhcp-snooping item(s) found  ---

```

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```

#
vlan 1
#
dhcp server ip-pool 0
network 10.1.1.0 mask 255.255.255.0
#
dhcp enable
#

```

- Switch B:

```

#
dhcp-snooping
#
vlan 1
arp detection enable
#
interface GigabitEthernet1/0/1
port link-mode bridge
dhcp-snooping trust
arp detection trust
#

```

DLDP configuration examples

This document provides DLDP configuration examples.

The Device Link Detection Protocol (DLDP) is developed by HP. DLDP detects unidirectional links (fiber links or twisted-pair links). When DLDP detects unidirectional links, it can automatically shut down the faulty port or users can manually shut down the faulty port to avoid network problems.

Example: Automatically shutting down unidirectional links

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

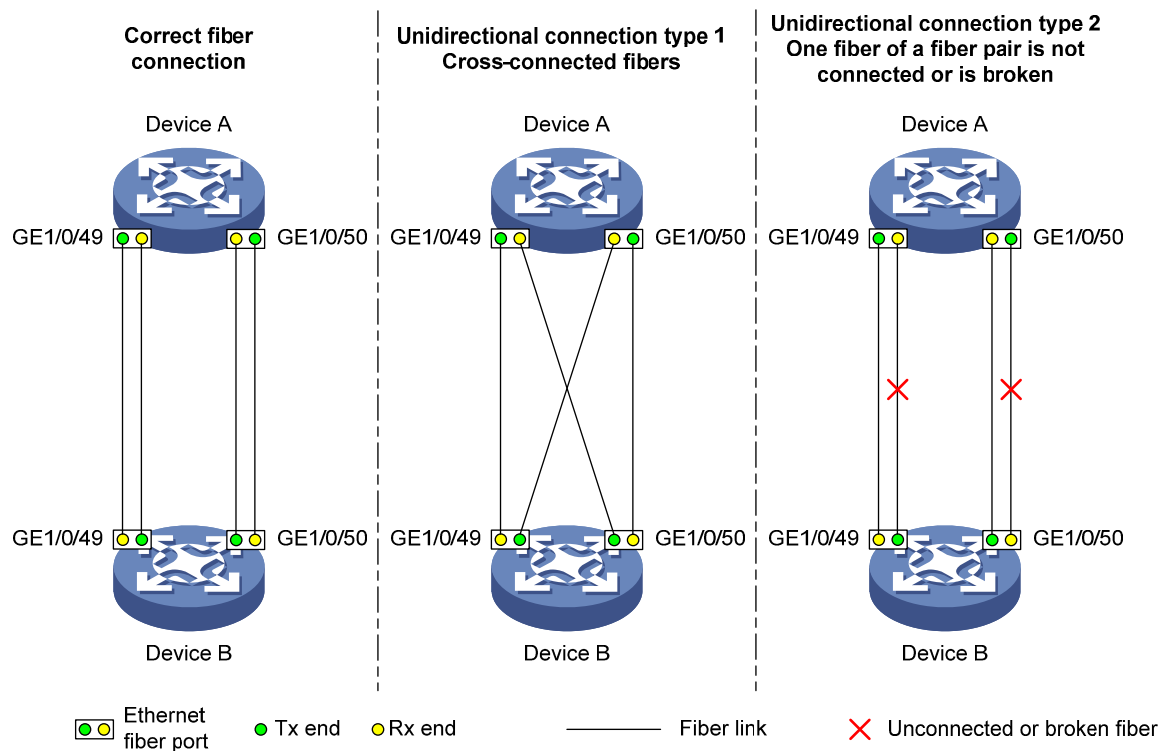
Network requirements

As shown in [Figure 57](#), Device A and Device B are connected with two fiber pairs.

Configure DLDP on the devices so each device performs these tasks:

- Detects unidirectional links caused by cross-connected fibers or a disconnected fiber or open circuit condition.
- Automatically shuts down the faulty port when detecting a unidirectional link.
- Automatically brings up the port after the administrator clears the fault.

Figure 57 Network diagram



Configuration restrictions and guidelines

When you configure DLDP, follow these restrictions and guidelines:

- To make sure DLDP operates correctly on a link, you must configure the full duplex mode for the ports at two ends of the link, and configure a speed for the two ports.
- The default DLDP mode is normal. The system can detect only unidirectional links caused by cross-connected fibers. To enable DLDP to detect unidirectional links caused by cross-connected fibers or a disconnected fiber or open circuit condition, set the DLDP mode to enhanced.

Configuration procedures

1. Configure Device A:

Enable DLDP globally.

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

Configure GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 to operate in full duplex mode at 1000 Mbps, and enable DLDP on the ports.

```
[DeviceA] interface gigabitethernet 1/0/49  
[DeviceA-GigabitEthernet1/0/49] duplex full  
[DeviceA-GigabitEthernet1/0/49] speed 1000
```

```

[DeviceA-GigabitEthernet1/0/49] dldp enable
[DeviceA-GigabitEthernet1/0/49] quit
[DeviceA] interface gigabitethernet 1/0/50
[DeviceA-GigabitEthernet1/0/50] duplex full
[DeviceA-GigabitEthernet1/0/50] speed 1000
[DeviceA-GigabitEthernet1/0/50] dldp enable
[DeviceA-GigabitEthernet1/0/50] quit

# Set the DLDP mode to enhanced.
[DeviceA] dldp work-mode enhance

# Set the port shutdown mode to auto.
[DeviceA] dldp unidirectional-shutdown auto

```

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

Verifying the configuration

Display the DLDP configuration information about all the DLDP-enabled ports of Device A.

```

[DeviceA] display dldp
DLDP global status : enable
DLDP interval : 5s
DLDP work-mode : enhance
DLDP authentication-mode : none
DLDP unidirectional-shutdown : auto
DLDP delaydown-timer : 1s
The number of enabled ports is 2.

Interface GigabitEthernet1/0/49
DLDP port state : advertisement
DLDP link state : up
The neighbor number of the port is 1.
    Neighbor mac address : 0023-8956-3600
    Neighbor port index : 59
    Neighbor state : two way
    Neighbor aged time : 11

Interface GigabitEthernet1/0/50
DLDP port state : advertisement
DLDP link state : up
The neighbor number of the port is 1.
    Neighbor mac address : 0023-8956-3600
    Neighbor port index : 60
    Neighbor state : two way
    Neighbor aged time : 12

```

The output shows that both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 are in Advertisement state, which means both links are bidirectional.

Enable system information monitoring on Device A, and enable the display of log and trap information.

```
[DeviceA] quit
<DeviceA> terminal monitor
Info: Current terminal monitor is on.
<DeviceA> terminal logging
Info: Current terminal logging is on.
<DeviceA> terminal trapping
Info: Current terminal trapping is on.
```

If the two pairs of fibers between Device A and Device B are cross-connected, the following log and trap information is displayed on Device A:

```
<DeviceA>
#Jan 18 17:36:18:798 2013 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1<hhpDLDPUnidirectionalPort> : DLDP detects a unidirectional
link in port 17825792.

%Jan 18 17:36:18:799 2013 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link status
is DOWN.

%Jan 18 17:36:18:799 2013 DeviceA DLDP/3/DLDP_UNIDIRECTION_AUTO: -Slot=1; DLDP detects
a unidirectional link on port GigabitEthernet1/0/49. The transceiver has malfunction in
the Tx direction or cross-connected links exist between the local device and its neighbor.
The shutdown mode is AUTO. DLDP shuts down the port.

#Jan 18 17:36:20:189 2013 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1<hhpDLDPUnidirectionalPort> : DLDP detects a unidirectional
link in port 17825793.

%Jan 18 17:36:20:189 2013 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link status
is DOWN.

%Jan 18 17:36:20:190 2013 DeviceA DLDP/3/DLDP_UNIDIRECTION_AUTO: -Slot=1; DLDP detects
a unidirectional link on port GigabitEthernet1/0/50. The transceiver has malfunction in
the Tx direction or cross-connected links exist between the local device and its neighbor.
The shutdown mode is AUTO. DLDP shuts down the port.

%Jan 15 16:54:56:040 2013 DeviceA DLDP/3/DLDP_UNIDIRECTION_AUTO_ENHANCE: -Slot=1; In
enhanced DLDP mode, port GigabitEthernet1/0/49 cannot detect its aged-out neighbor. The
transceiver has malfunction in the Tx direction or cross-connected links exist between
the local device and its neighbor. The shutdown mode is AUTO. DLDP shuts down the port.
```

The output shows that the link status of both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 is down, and DLDP has detected a unidirectional link on both ports and has automatically shut them down.

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

```
<DeviceA>
%Jan 18 17:47:33:869 2013 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link status
is UP.
%Jan 18 17:47:35:894 2013 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link status
is UP.
```

The output shows that the link status of both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 is now up.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```
#
dldp enable
dldp work-mode enhance
#
interface GigabitEthernet1/0/49
port link-mode bridge
speed 1000
duplex full
dldp enable
#
interface GigabitEthernet1/0/50
port link-mode bridge
speed 1000
duplex full
dldp enable
#
```

- Device B:

The configuration files on Device B are the same as those on Device A. (Details not shown.)

Example: Manually shutting down unidirectional links

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

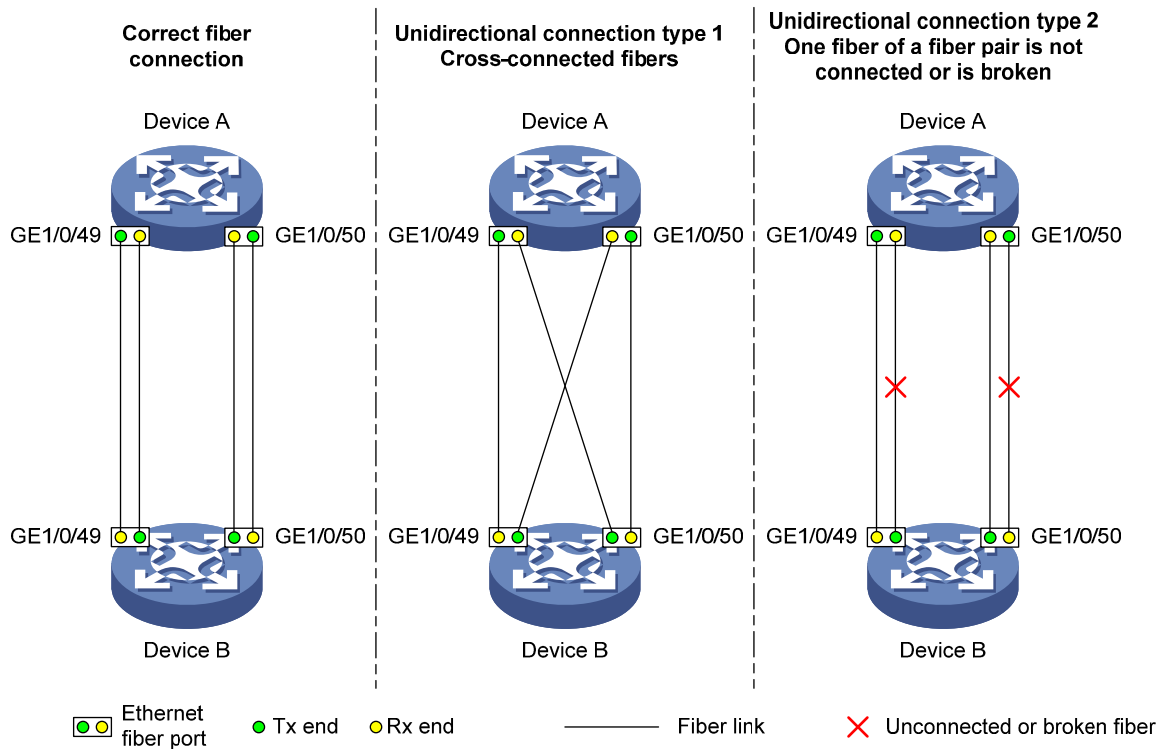
As shown in [Figure 58](#), Device A and Device B are connected with two fiber pairs.

Configure DLDP on the devices to meet these requirements:

- Each device can 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 58 Network diagram



Configuration restrictions and guidelines

When you configure DLDAP, follow these restrictions and guidelines:

- To make sure DLDAP operates correctly on a link, you must configure the full duplex mode for the ports at two ends of the link, and configure a speed for the two ports.
- The default DLDAP mode is normal. The system can detect only unidirectional links caused by cross-connected fibers. To enable DLDAP to detect unidirectional links caused by cross-connected fibers or a disconnected fiber or open circuit condition, set the DLDAP mode to enhanced.

Configuration procedures

1. Configure Device A:

Enable DLDAP globally.

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

Configure GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 to operate in full duplex mode at 1000 Mbps, and enable DLDAP on the ports.

```
[DeviceA] interface gigabitethernet 1/0/49
```

```

[DeviceA-GigabitEthernet1/0/49] duplex full
[DeviceA-GigabitEthernet1/0/49] speed 1000
[DeviceA-GigabitEthernet1/0/49] dldp enable
[DeviceA-GigabitEthernet1/0/49] quit
[DeviceA] interface gigabitethernet 1/0/50
[DeviceA-GigabitEthernet1/0/50] duplex full
[DeviceA-GigabitEthernet1/0/50] speed 1000
[DeviceA-GigabitEthernet1/0/50] dldp enable
[DeviceA-GigabitEthernet1/0/50] quit

# Set the DLDAP mode to enhanced.
[DeviceA] dldp work-mode enhance

# Set the port shutdown mode to manual.
[DeviceA] dldp unidirectional-shutdown manual

```

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

Verifying the configuration

- # Display the DLDAP configuration information on all the DLDAP-enabled ports of Device A.

```

[DeviceA] display dldp
DLDP global status : enable
DLDP interval : 5s
DLDP work-mode : enhance
DLDP authentication-mode : none
DLDP unidirectional-shutdown : manual
DLDP delaydown-timer : 1s
The number of enabled ports is 2.

Interface GigabitEthernet1/0/49
DLDP port state : advertisement
DLDP link state : up
The neighbor number of the port is 1.
    Neighbor mac address : 0023-8956-3600
    Neighbor port index : 59
    Neighbor state : two way
    Neighbor aged time : 11

```

```

Interface GigabitEthernet1/0/50
DLDP port state : advertisement
DLDP link state : up
The neighbor number of the port is 1.
    Neighbor mac address : 0023-8956-3600
    Neighbor port index : 60
    Neighbor state : two way
    Neighbor aged time : 12

```

The output shows that both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 are in Advertisement state, which means both links are bidirectional.

Enable system information monitoring on Device A, and enable the display of log and trap information.

```
[DeviceA] quit
<DeviceA> terminal monitor
Info: Current terminal monitor is on.
<DeviceA> terminal logging
Info: Current terminal logging is on.
<DeviceA> terminal trapping
Info: Current terminal trapping is on.
```

If the two pairs of fibers between Device A and Device B are cross-connected, the following log and trap information is displayed on Device A:

```
<DeviceA>
#Jan 18 18:10:38:481 2013 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1<hhpDLDPUnidirectionalPort> : DLDP detects a unidirectional
link in port 17825792.

%Jan 18 18:10:38:481 2013 DeviceA DLDP/3/DLDP_UNIDIRECTION_MANUAL: -Slot=1; DLDP detects
a unidirectional link on port GigabitEthernet1/0/49. The transceiver has malfunction in
the Tx direction or cross-connected links exist between the local device and its neighbor.
The shutdown mode is MANUAL. The port needs to be shut down by the user.

#Jan 18 18:10:38:618 2013 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1<hhpDLDPUnidirectionalPort> : DLDP detects a unidirectional
link in port 17825793.

%Jan 18 18:10:38:618 2013 DeviceA DLDP/3/DLDP_UNIDIRECTION_MANUAL: -Slot=1; DLDP detects
a unidirectional link on port GigabitEthernet1/0/50. The transceiver has malfunction in
the Tx direction or cross-connected links exist between the local device and its neighbor.
The shutdown mode is MANUAL. The port needs to be shut down by the user.
```

The output shows that DLDP has detected a unidirectional link on both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50, and is asking you to manually shut down the faulty ports.

Shut down GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/49
[DeviceA-GigabitEthernet1/0/49] shutdown
%Jan 18 18:16:12:044 2010 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link status
is DOWN.
[DeviceA-GigabitEthernet1/0/49] quit
[DeviceA] interface gigabitethernet 1/0/50
[DeviceA-GigabitEthernet1/0/50] shutdown
%Jan 18 18:18:03:583 2010 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link status
is DOWN.
```

The output shows that the link status of both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 is down.

In this example, the unidirectional links are caused by cross-connected fibers.

Correct the fiber connections, and then bring up GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 that are previously shut down on Device A.

```

[DeviceA-GigabitEthernet1/0/50] undo shutdown
[DeviceA-GigabitEthernet1/0/50]
%Jan 18 18:22:11:698 2010 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link status
is UP.
[DeviceA-GigabitEthernet1/0/50] quit
[DeviceA] interface gigabitethernet 1/0/49
[DeviceA-GigabitEthernet1/0/49] undo shutdown
[DeviceA-GigabitEthernet1/0/49]
%Jan 18 18:22:46:065 2010 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link status
is UP.

```

The output shows that the link status of both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 is now up.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```

#
 dldp enable
 dldp work-mode enhance
 dldp unidirectional-shutdown manual
#
interface GigabitEthernet1/0/49
 port link-mode bridge
 speed 1000
 duplex full
 dldp enable
#
interface GigabitEthernet1/0/50
 port link-mode bridge
 speed 1000
 duplex full
 dldp enable
#

```

- Device B:

The configuration files on Device B are the same as those on Device A. (Details not shown.)

DNS configuration examples

This document provides DNS configuration examples.

Example: Configuring IPv4 static DNS

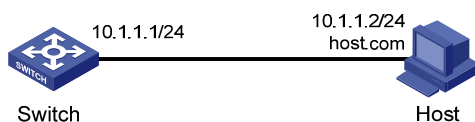
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 59](#), configure IPv4 static DNS so the switch can access Host by using the domain name **host.com** rather than an IP address.

Figure 59 Network diagram



Configuration procedures

```
# Create a mapping between host name host.com and IP address 10.1.1.2.  
<Switch> system-view  
[Switch] ip host host.com 10.1.1.2
```

Verifying the configuration

Use the **ping host.com** command on the switch. The output shows that the switch can use static domain name resolution to resolve domain name **host.com** into IP address 10.1.1.2.

```
<Switch> ping host.com  
PING host.com (10.1.1.2):  
56 data bytes, press CTRL_C to break  
Reply from 10.1.1.2: bytes=56 Sequence=0 ttl=128 time=2 ms
```

```

Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=128 time=2 ms
Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=128 time=2 ms
Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=128 time=2 ms
Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=128 time=2 ms

--- host.com ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 2/2/2 ms

```

Configuration files

```

#
ip host host.com 10.1.1.2
#

```

Example: Configuring IPv4 dynamic DNS

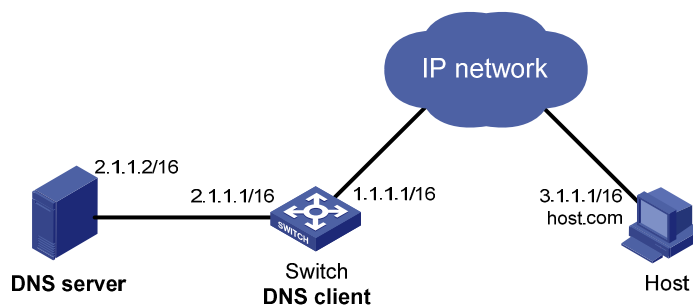
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 60](#), 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 60 Network diagram



Configuration procedures

Configuring the DNS server

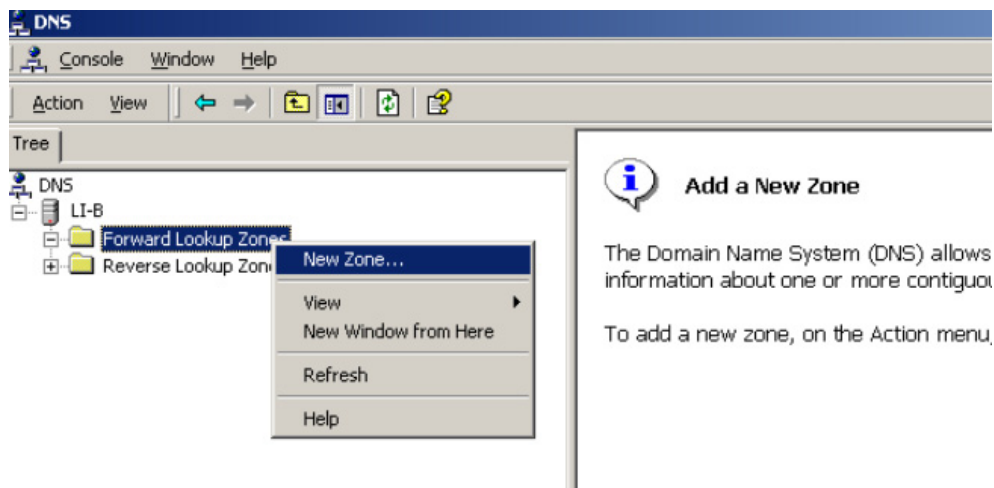
The configuration might vary with DNS servers. The following configuration is performed on a PC running Windows Server 2000.

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

The DNS server configuration page appears, as shown in [Figure 61](#).

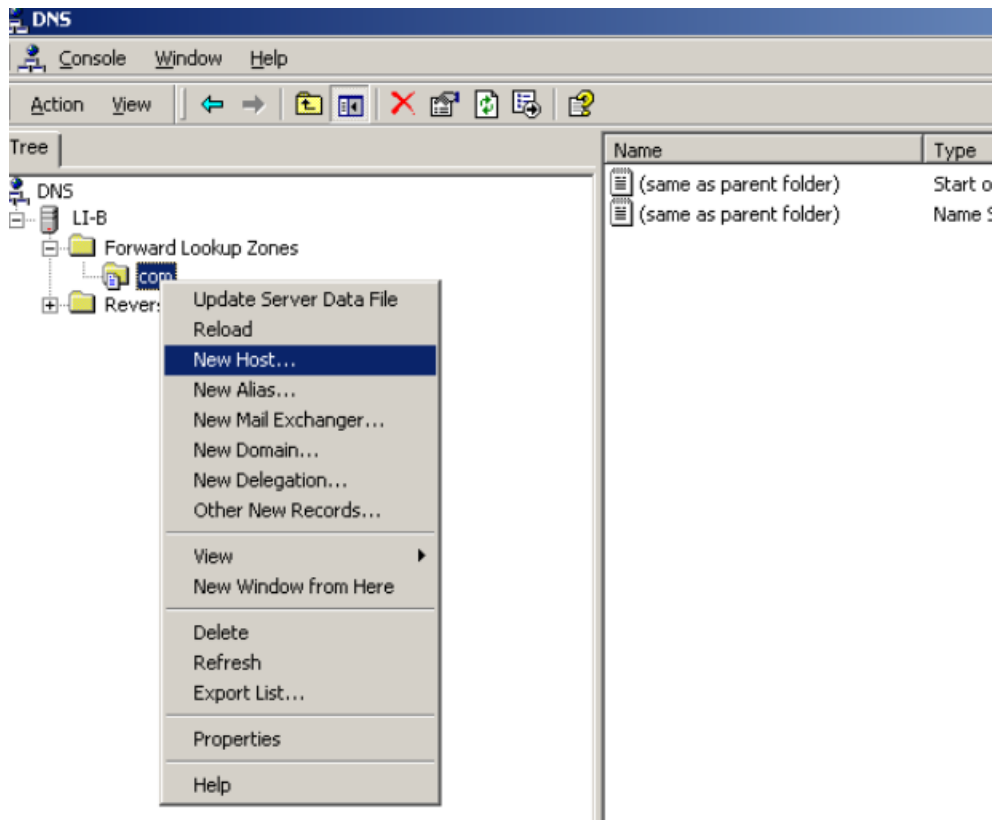
2. Right-click **Forward Lookup Zones**, select **New Zone**, and then follow the wizard to create a new zone named **com**.

Figure 61 Creating a zone



3. On the DNS server configuration page, right-click zone **com** and select **New Host**.

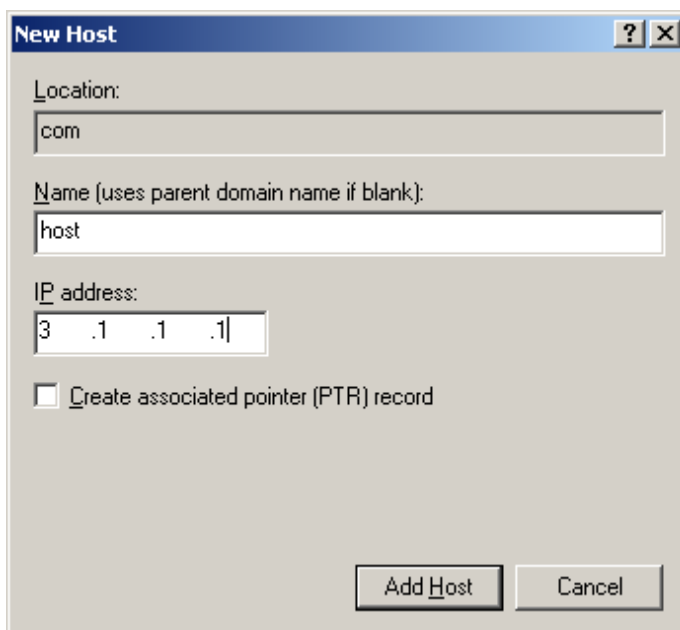
Figure 62 Adding a host



4. On the page that appears, enter host name **host** and IP address **3.1.1.1**.
5. Click **Add Host**.

The mapping between the IP address and host name is created.

Figure 63 Adding a mapping between domain name and IP address



Configuring the switch

```
# Enable dynamic domain name resolution.
<Switch> system-view
[Switch] dns resolve

# Specify the IP address of the DNS server as 2.1.1.2.
[Switch] dns server 2.1.1.2

# Specify com as the name suffix.
[Switch] dns domain com
```

Verifying the configuration

Use the **ping host** command on the switch. The output shows that the ping operation succeeds, and that the translated destination IP address is 3.1.1.1.

```
<Switch> ping host
Trying DNS resolve, press CTRL_C to break
Trying DNS server (2.1.1.2)
PING host.com (3.1.1.1):
 56 data bytes, press CTRL_C to break
  Reply from 3.1.1.1: bytes=56 Sequence=0 ttl=126 time=3 ms
  Reply from 3.1.1.1: bytes=56 Sequence=1 ttl=126 time=1 ms
  Reply from 3.1.1.1: bytes=56 Sequence=2 ttl=126 time=1 ms
  Reply from 3.1.1.1: bytes=56 Sequence=3 ttl=126 time=1 ms
  Reply from 3.1.1.1: bytes=56 Sequence=4 ttl=126 time=1 ms

--- host.com ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/3 ms
```

Configuration files

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

Example: Configuring IPv4 DNS

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 64](#), Switch A, the DNS server, Switch C, and the host can reach each other.

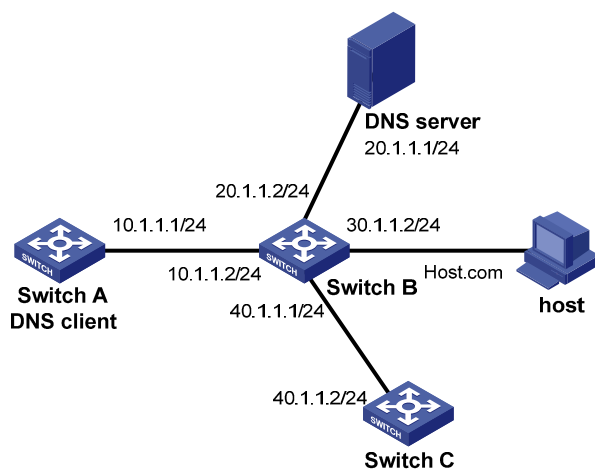
Switch A is attempting to access the following devices:

- Switch C at a fixed IP address.
- 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 64 Network diagram



Configuration procedures

Configuring the DNS server

For information about the DNS server configuration, see "[Example: Configuring IPv4 dynamic DNS.](#)"

Configuring Switch A

Create a mapping between IP address 40.1.1.2 and domain name **SwitchC**.

```
<SwitchA> system-view
[SwitchA] ip host SwitchC 40.1.1.2
```

Enable dynamic domain name resolution.

```
[SwitchA] dns resolve
```

Specify the IP address of the DNS server as 20.1.1.1.

```
[SwitchA] dns server 20.1.1.1
```

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

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

Verifying the configuration

Use the **ping SwitchC** command on Switch A. The output shows that Switch A can use static domain name resolution to resolve domain name **SwitchC** into IP address **40.1.1.2**.

```
<SwitchA> ping SwitchC
PING SwitchC (40.1.1.2):
 56 data bytes, press CTRL_C to break
  Reply from 40.1.1.2: bytes=56 Sequence=1 ttl=126 time=2 ms
  Reply from 40.1.1.2: bytes=56 Sequence=2 ttl=126 time=2 ms
  Reply from 40.1.1.2: bytes=56 Sequence=3 ttl=126 time=2 ms
  Reply from 40.1.1.2: bytes=56 Sequence=4 ttl=126 time=2 ms
  Reply from 40.1.1.2: bytes=56 Sequence=5 ttl=126 time=2 ms

--- SwitchC ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 2/2/2 ms
```

Use the **ping host** command on Switch A. The output shows that the ping operation succeeds, and that the translated destination IP address is 3.1.1.1.

```
[SwitchA] ping host
Trying DNS resolve, press CTRL_C to break
Trying DNS server (20.1.1.1)
PING host.com (30.1.1.1):
 56 data bytes, press CTRL_C to break
  Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=126 time=3 ms
  Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=126 time=1 ms
  Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=126 time=1 ms
  Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=126 time=1 ms
  Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=126 time=1 ms

--- host.com ping statistics ---
 5 packet(s) transmitted
```

```
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/1/3 ms
```

Configuration files

```
#
dns resolve
dns server 20.1.1.1
dns domain com
#
ip host host.com 40.1.1.2
#
```

Example: Configuring IPv6 static DNS

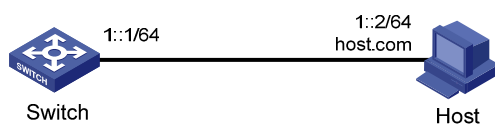
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 65](#), configure IPv6 static DNS so the switch can access the host by using the domain name **host.com** rather than an IPv6 address.

Figure 65 Network diagram



Configuration procedures

```
# Create a mapping between domain name host.com and IPv6 address 1::2.
<Switch> system-view
[Switch] ipv6 host host.com 1::2

# Enable IPv6.
[Switch] ipv6
```

Verifying the configuration

Use the **ping ipv6 host.com** command on the switch. The output shows that the switch can use static domain name resolution to resolve domain name **host.com** into IPv6 address **1::2**.

```
<Switch> ping ipv6 host.com
  PING host.com (1::2):
  56 data bytes, press CTRL_C to break
  Reply from 1::2
  bytes=56 Sequence=0 hop limit=64  time = 3 ms
  Reply from 1::2
  bytes=56 Sequence=1 hop limit=64  time = 1 ms
  Reply from 1::2
  bytes=56 Sequence=2 hop limit=64  time = 1 ms
  Reply from 1::2
  bytes=56 Sequence=3 hop limit=64  time = 2 ms
  Reply from 1::2
  bytes=56 Sequence=4 hop limit=64  time = 2 ms
--- host.com ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/1/3 ms
```

Configuration files

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

Example: Configuring IPv6 dynamic DNS

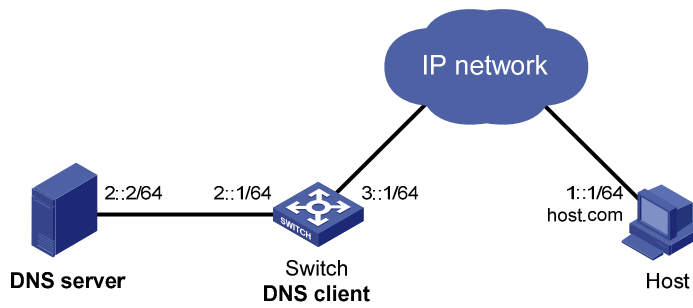
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 66](#), 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 66 Network diagram



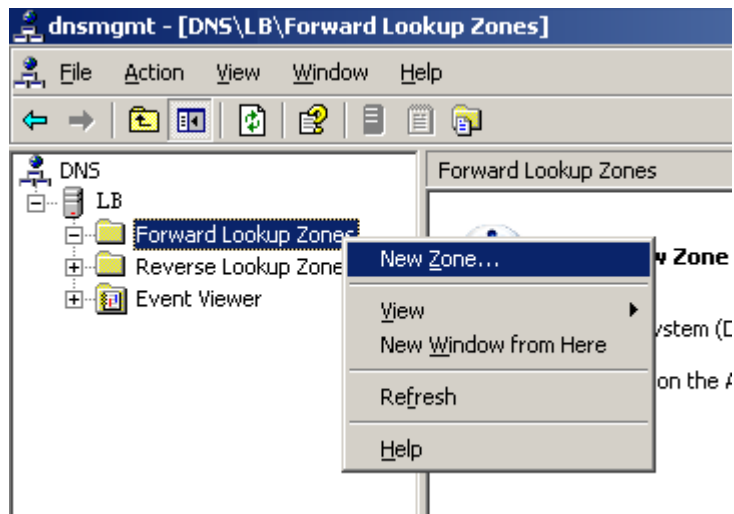
Configuration procedures

Configuring the DNS server

This configuration might vary with DNS servers. The following configuration is performed on a PC running Windows Server 2003.

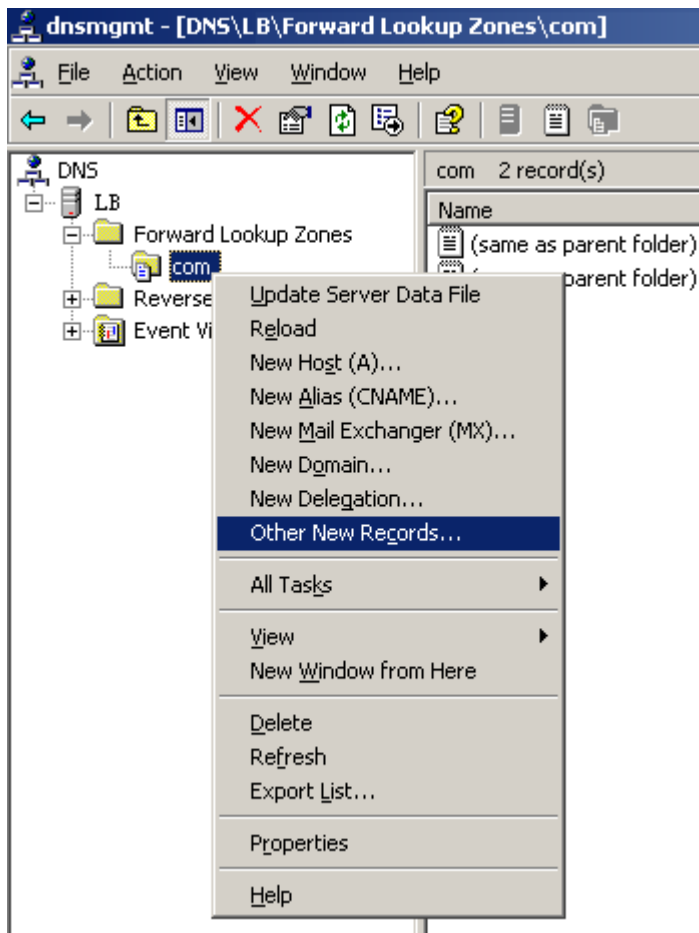
1. Select **Start > Programs > Administrative Tools > DNS**.
The DNS server configuration page appears, as shown in [Figure 67](#).
2. Right-click **Forward Lookup Zones**, select **New Zone**, and then follow the wizard to create a new zone named **com**.

Figure 67 Creating a zone



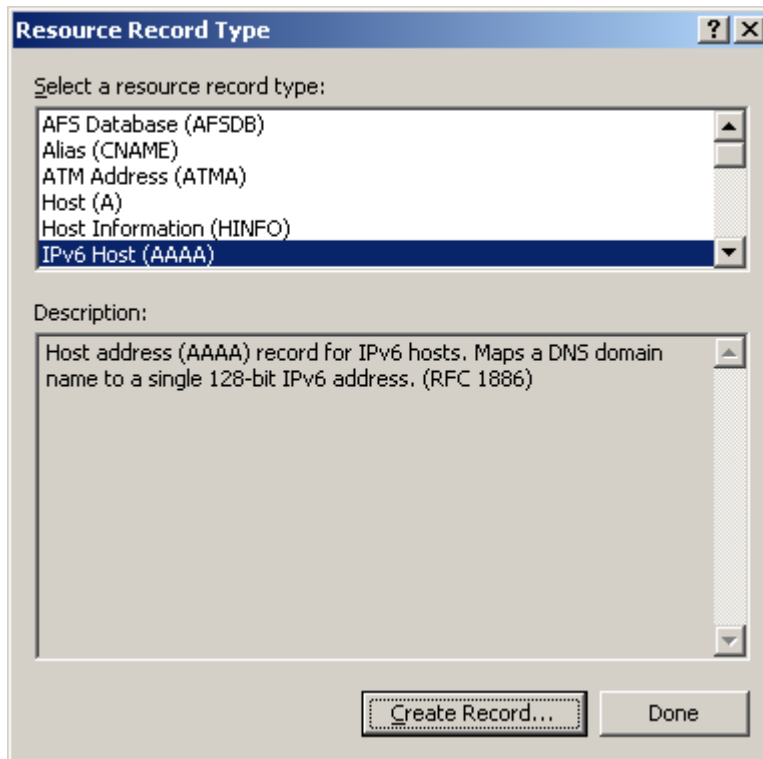
3. On the DNS server configuration page, right-click zone **com**, and select **Other New Records**.

Figure 68 Creating a record



4. On the page that appears, select **IPv6 Host (AAAA)** as the resource record type.

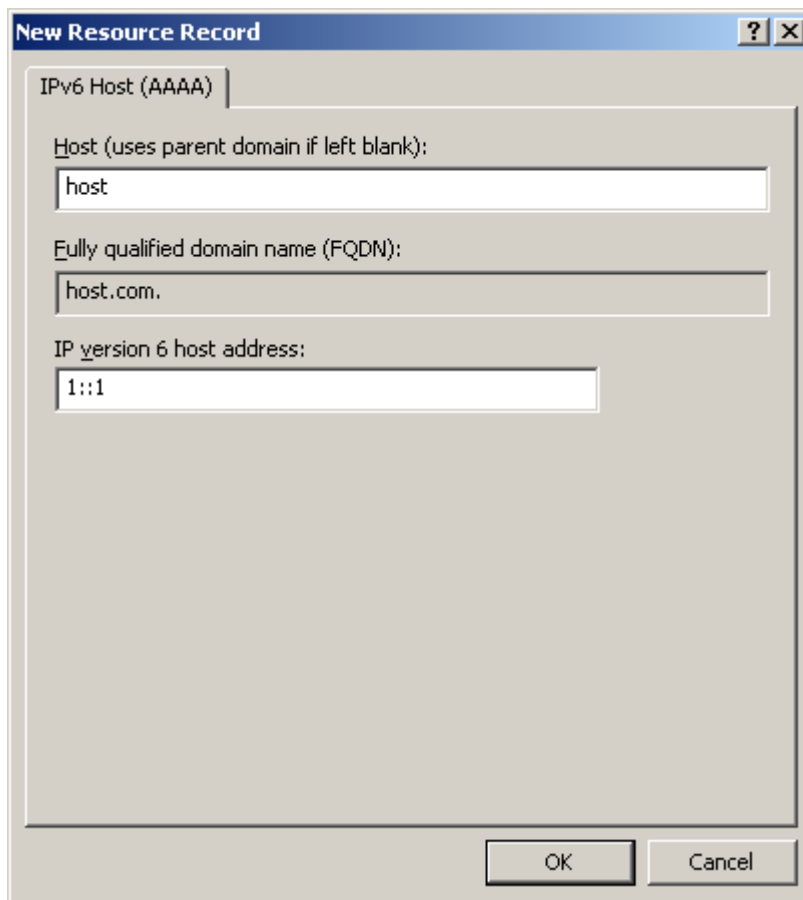
Figure 69 Selecting the resource record type



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 70 Adding a mapping between the domain name and IPv6 address



Configuring the Switch

Enable dynamic domain name resolution.

```
<Switch> system-view  
[Switch] dns resolve
```

Enable IPv6.

```
[Switch] ipv6
```

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

```
[Switch] dns server ipv6 2::2
```

Specify **com** as the DNS suffix.

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

Verifying the configuration

Use the **ping ipv6 host** command on the switch. The output shows that the ping operation succeeds, and that the translated destination IP address is 1::1.

```
<Switch> ping ipv6 host  
Trying DNS resolve, press CTRL_C to break
```

```

Trying DNS server (2::2)
PING host.com (1::1):
56 data bytes, press CTRL_C to break
  Reply from 1::1
    bytes=56 Sequence=0 hop limit=60  time = 2 ms
  Reply from 1::1
    bytes=56 Sequence=1 hop limit=60  time = 1 ms
  Reply from 1::1
    bytes=56 Sequence=2 hop limit=60  time = 1 ms
  Reply from 1::1
    bytes=56 Sequence=3 hop limit=60  time = 1 ms
  Reply from 1::1
    bytes=56 Sequence=4 hop limit=60  time = 1 ms

--- host.com ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/1/2 ms

```

Configuration files

```

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

```

Example: Configuring IPv6 DNS

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 71](#), Switch A, the DNS server, Switch C, and the host can reach each other.

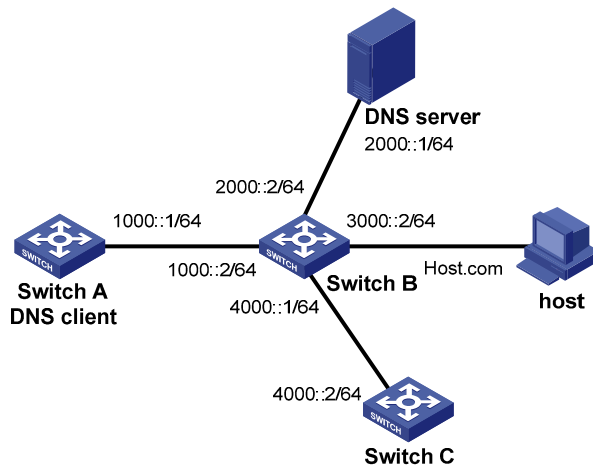
Switch A is attempting to access the following devices:

- Switch C at a fixed IPv6 address.
- 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 71 Network diagram



Configuration procedures

Configuring the DNS server

For information about the DNS server configuration, see "[Example: Configuring IPv6 dynamic DNS.](#)"

Configuring Switch A

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

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

Enable IPv6.

```
[SwitchA] ipv6
```

Enable dynamic domain name resolution.

```
[SwitchA] dns resolve
```

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

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

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

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

Verifying the configuration

Use the **ping SwitchC** command on Switch A. The output shows that Switch A can use static domain name resolution to resolve domain name **SwitchC** into IP address **4000::2**.

```
<SwitchA> ping ipv6 SwitchC
PING SwitchC (1::2):
 56 data bytes, press CTRL_C to break
  Reply from 1::2
  bytes=56 Sequence=0 hop limit=63  time = 3 ms
  Reply from 1::2
  bytes=56 Sequence=1 hop limit=63  time = 1 ms
  Reply from 1::2
  bytes=56 Sequence=2 hop limit=63  time = 1 ms
  Reply from 1::2
  bytes=56 Sequence=3 hop limit=63  time = 2 ms
  Reply from 1::2
  bytes=56 Sequence=4 hop limit=63  time = 2 ms
--- SwitchC ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/3 ms
```

Use the **ping host** command on Switch A. The output shows that the ping operation succeeds, and that the translated destination IP address is **3000::1**.

```
[SwitchA] ping ipv6 host
Trying DNS resolve, press CTRL_C to break
Trying DNS server (2000::1)
PING host.com (3000::1):
 56 data bytes, press CTRL_C to break
  Reply from 3000::1
  bytes=56 Sequence=0 hop limit=63  time = 2 ms
  Reply from 3000::1
  bytes=56 Sequence=1 hop limit=63  time = 1 ms
  Reply from 3000::1
  bytes=56 Sequence=2 hop limit=63  time = 1 ms
  Reply from 3000::1
  bytes=56 Sequence=3 hop limit=63  time = 1 ms
  Reply from 3000::1
  bytes=56 Sequence=4 hop limit=63  time = 1 ms
--- host.com ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/2 ms
```

Configuration files

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

Ethernet OAM configuration examples

This document provides Ethernet OAM configuration examples.

Ethernet OAM is a tool that monitors the status of the link between two directly connected switches.

Example: Configuring Ethernet OAM

Applicable product matrix

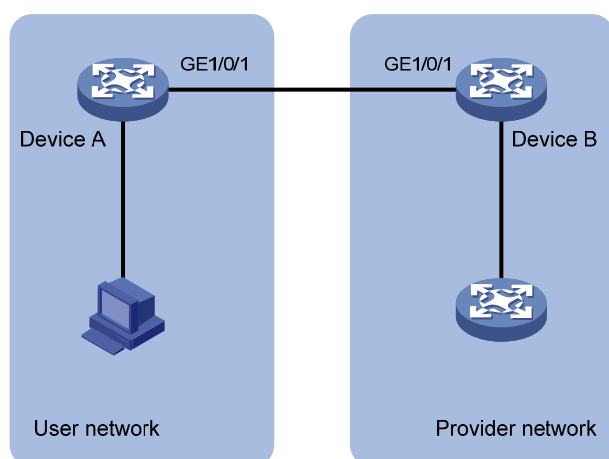
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 72](#), 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 72 Network diagram



Requirement analysis

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

Configuration procedures

1. Configure Device A:

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

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

2. Configure Device B:

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

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

# Enable Ethernet OAM for the port.
[DeviceB-GigabitEthernet1/0/1] oam enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display the Ethernet OAM configuration on Device A.

```
[DeviceA] display oam configuration
Configuration of the link event window/threshold :
-----
Errored-symbol Event period(in seconds)      :      1
Errored-symbol Event threshold                :      1
Errored-frame Event period(in seconds)       :      1
Errored-frame Event threshold                :      1
Errored-frame-period Event period(in ms)     :    1000
Errored-frame-period Event threshold         :      1
Errored-frame-seconds Event period(in seconds) :     60
Errored-frame-seconds Event threshold       :      1

Configuration of the timer :
-----
Hello timer(in ms)                          :    1000
```

```
Keepalive timer(in ms) : 5000
```

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

```
[DeviceB] display oam link-event remote
```

```
Port :GigabitEthernet1/0/1
```

```
Link Status :Up
```

```
OAMRemoteErrFrameEvent : (ms = milliseconds)
```

```
-----  
Event Time Stamp      : 5789      Errored FrameWindow : 10(100ms)  
Errored Frame Threshold : 1      Errored Frame       : 3  
Error Running Total   : 35      Event Running Total : 17
```

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

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```
#  
interface GigabitEthernet1/0/1  
  port link-mode bridge  
  oam mode passive  
  oam enable
```

- Device B:

```
#  
interface GigabitEthernet1/0/1  
  port link-mode bridge  
  oam enable
```

HABP configuration examples

This chapter provides HABP configuration examples for the downstream network devices of an 802.1X or MAC authentication-enabled device to bypass authentication.

Example: Configuring HABP

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

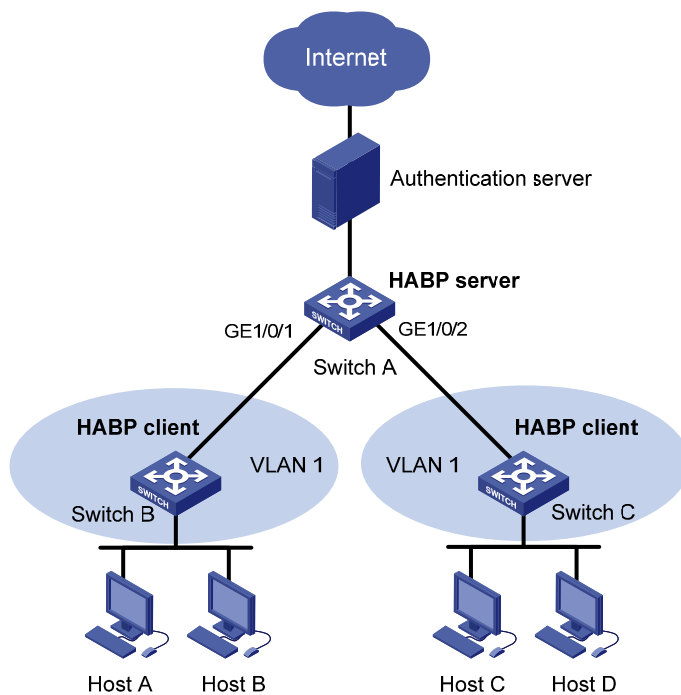
Network requirements

As shown in [Figure 73](#), Switch A is connected to downstream access devices Switch B and Switch C.

Configure the switches to meet the following requirements:

- Configure 802.1X authentication on Switch A for central authentication and management of users (Host A through Host D).
- Configure HABP on Switch A, Switch B, and Switch C to allow Switch B and Switch C to bypass 802.1X authentication.

Figure 73 Network diagram



Requirements analysis

For communication between Switch B and Switch C, you must perform the following tasks:

- Enable HABP server on Switch A.
- Enable HABP client on Switch B and Switch C.
- Specify VLAN 1 for HABP packets.

Configure the HABP server to send HABP request packets to the HABP clients in VLAN 1 at a correct interval depending on the network conditions.

Configuration restrictions and guidelines

The VLAN specified on the HABP server must be the same as the VLAN to which the HABP clients belong.

Configuration procedures

Configuring Switch A

Configure 802.1X. For more information, see "802.1X configuration examples."

Enable HABP on the switch. By default, HABP is enabled.

```
<SwitchA> system-view  
[SwitchA] habp enable
```

```
# Configure HABP to operate in server mode, and specify VLAN 1 for HABP packets.
```

```
[SwitchA] habp server vlan 1
```

```
# Specify the switch to send HABP request packets at 50-second intervals.
```

```
[SwitchA] habp timer 50
```

Configuring Switch B

```
# Enable HABP on the switch. By default, HABP is enabled.
```

```
<SwitchA> system-view
```

```
[SwitchB] habp enable
```

```
# Configure HABP to operate in client mode. By default, HABP operates in client mode.
```

```
[SwitchB] undo habp server
```

```
# Specify the HABP client to belong to VLAN 1. By default, HABP client belongs to VLAN 1.
```

```
[SwitchB] habp client vlan 1
```

Configuring Switch C

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

Verifying the configuration

```
# Display HABP configuration.
```

```
<SwitchA> display habp
```

```
Global HABP information:
```

```
    HABP Mode: Server
```

```
    Sending HABP request packets every 50 seconds
```

```
    Bypass VLAN: 1
```

```
# Display HABP MAC address table entries.
```

```
<SwitchA> display habp table
```

MAC	Holdtime	Receive Port
001f-3c00-0030	53	GigabitEthernet1/0/2
001f-3c00-0031	53	GigabitEthernet1/0/1

Configuration files

```
Switch A:
```

```
#
```

```
    habp server vlan 1
```

```
    habp timer 50
```

```
#
```

IGMP configuration examples

This chapter provides examples for configuring IGMP to manage IP multicast group membership.

General configuration restrictions and guidelines

When you configure IGMP, follow these restrictions and guidelines:

- Do not enable IGMP on a VLAN interface that is running a Layer 2 multicast protocol.
- Do not enable IGMP proxying on a VLAN interface that is enabled with IGMP snooping.
- Do not enable IGMP on an interface that is enabled with IGMP proxying.

Example: Configuring multicast group filters

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

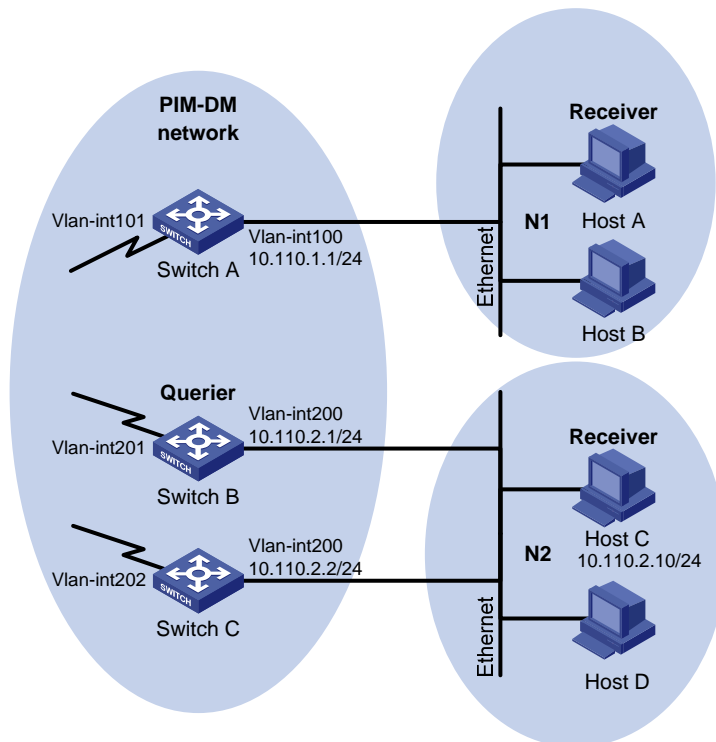
Network requirements

As shown in [Figure 74](#):

- 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 74 Network diagram



Requirements analysis

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, create a basic ACL, specifying the range of the multicast groups that host receivers 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 74](#). (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, and specify the range of the multicast groups that host receivers 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 PIM-DM on VLAN-interface 200.
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp enable
[SwitchB-Vlan-interface200] pim dm
# Configure a multicast group filter that references ACL 2001 on VLAN-interface 200.
[SwitchB-Vlan-interface200] igmp group-policy 2001
[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, and specify the range of the multicast groups that host receivers 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 PIM-DM on VLAN-interface 200.
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] igmp enable
[SwitchC-Vlan-interface200] pim dm
# Configure a multicast group filter that references ACL 2001 on VLAN-interface 200.

```

```
[SwitchC-Vlan-interface200] igmp group-policy 2001
[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
Interface information of VPN-Instance: public net
Vlan-interface200(10.110.2.1):
  IGMP is enabled
  Current IGMP version is 2
  Value of query interval for IGMP(in seconds): 60
  Value of other querier present interval for IGMP(in seconds): 125
  Value of maximum query response time for IGMP(in seconds): 10
  Querier for IGMP: 10.110.2.1 (this router)
  Total 1 IGMP Group reported
```

Display information about the IGMP querier on Switch C.

```
[SwitchC] display igmp interface
Interface information of VPN-Instance: public net
Vlan-interface200(10.110.2.2):
  IGMP is enabled
  Current IGMP version is 2
  Value of query interval for IGMP(in seconds): 60
  Value of other querier present interval for IGMP(in seconds): 125
  Value of maximum query response time for IGMP(in seconds): 10
  Querier for IGMP: 10.110.2.1
  Total 1 IGMP Group reported
```

The output shows that Switch B, with the smaller IP address, has become the IGMP querier on this media-shared subnet.

2. Send IGMP reports from Host C in N2 to join the multicast groups **224.1.1.1** and **224.1.1.2**. (Details not shown.)
3. Display information about IGMP groups:

Display information about IGMP groups on Switch B.

```
[SwitchB] display igmp group
Total 1 IGMP Group(s).
Interface group report information of VPN-Instance: public net
Vlan-interface200(10.110.2.1):
  Total 1 IGMP Groups reported
  Group Address    Last Reporter    Uptime          Expires
```

```
224.1.1.1      10.110.2.10    04:36:03    00:01:23
```

Display information about IGMP groups on Switch C.

```
[SwitchC] display igmp group
```

```
Total 1 IGMP Group(s).
```

```
Interface group report information of VPN-Instance: public net
```

```
Vlan-interface200(10.110.2.2):
```

```
Total 1 IGMP Groups reported
```

Group Address	Last Reporter	Uptime	Expires
224.1.1.1	10.110.2.10	04:21:03	00:01:13

The output shows that only information about the multicast group 224.1.1.1 is displayed on Switch B and Switch C. 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
igmp enable
pim dm
#
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
igmp enable
igmp group-policy 2001
pim dm
#
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
  igmp enable
  igmp group-policy 2001
  pim dm
#
 interface Vlan-interface202
  pim dm
#

```

Example: Configuring IGMP SSM mappings

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

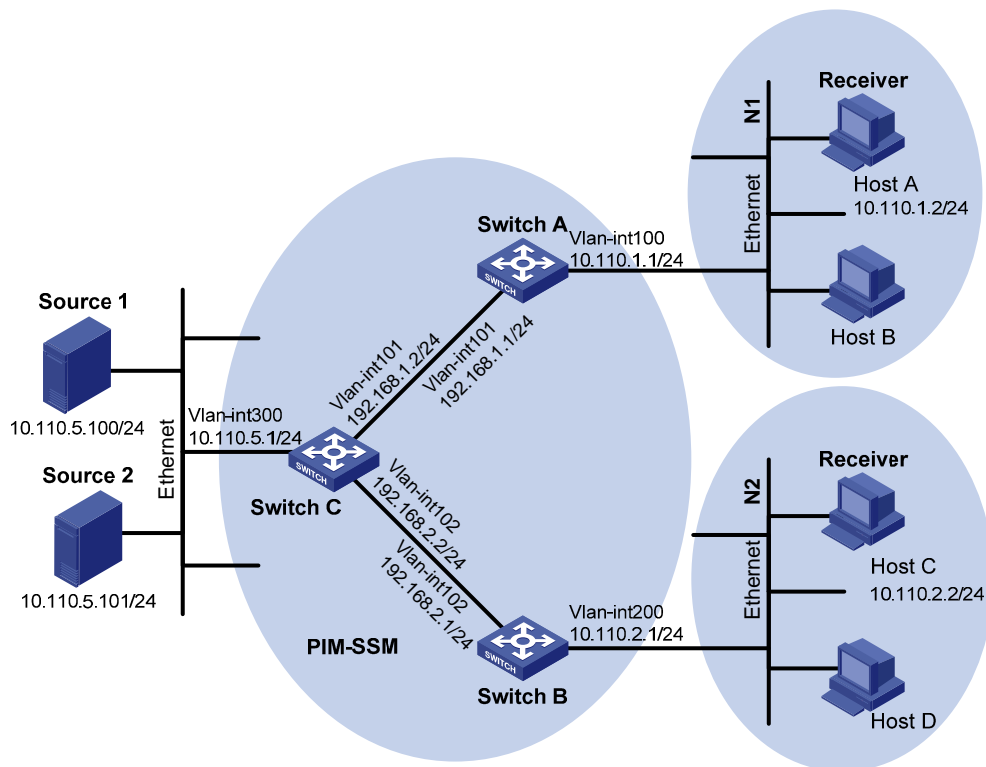
Network requirements

As shown in [Figure 75](#):

- The PIM-SSM network provides services for the multicast groups in the range of 232.1.1.0/24.
- Edge switches of N1 and N2 are running IGMPv3.
- Host A and Host C support IGMPv1 and IGMPv2, but do not support IGMPv3.
- All switches run OSPF, and they can communicate with each other through unicast routes.

Configure IGMP SSM mappings so that Host A and Host C receive multicast data from Source 1 and Source 2, respectively.

Figure 75 Network diagram



Configuration restrictions and guidelines

When you configure IGMP SSM mapping, follow these restrictions and guidelines:

- The IGMP SSM mapping does not process IGMPv3 reports.
- To display information about the multicast groups created based on the configured IGMP SSM mappings, use the **display igmp ssm-mapping group** command. Do not use the **display igmp group** command.

Configuration procedures

1. Assign an IP address and subnet mask to each interface, as shown in Figure 75. (Details not shown.)
2. Enable OSPF on all switches on the PIM-SSM network. (Details not shown)
3. Enable IP multicast routing and PIM-SM:

On Switch A, enable IP multicast routing globally, and enable PIM-SM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
```

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
```

Enable IP multicast routing and PIM-SM on Switch B and Switch C in the same way Switch A is configured. (Details not shown.)

4. Enable IGMPv3 on interfaces that connect N1 and N2:

Enable IGMPv3 on VLAN-interface 100 of Switch A. (By default, the IGMP version is 2.)

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] igmp version 3
[SwitchA-Vlan-interface100] quit
```

Enable IGMPv3 on Switch B in the same way Switch A is configured. (Details not shown.)

5. Specify the SSM multicast group address range:

On Switch A, specify the SSM multicast group address range as 232.1.1.0/24.

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[SwitchA-acl-basic-2000] quit
[SwitchA] pim
[SwitchA-pim] ssm-policy 2000
[SwitchA-pim] quit
```

Specify the same SSM multicast group address range on Switch B and Switch C in the same way Switch A is configured. (Details not shown.)

6. Enable IGMP SSM mapping and configure IGMP SSM mappings:

On Switch A, enable IGMP SSM mapping on VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp ssm-mapping enable
[SwitchA-Vlan-interface100] quit
```

On Switch A, configure an IGMP SSM mapping for the multicast source (Source 1) and multicast groups in the range of 232.1.1.0/24.

```
[SwitchA] igmp
[SwitchA-igmp] ssm-mapping 232.1.1.0 24 10.110.5.100
[SwitchA-igmp] quit
```

On Switch B, enable IGMP SSM mapping on VLAN-interface 200.

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp ssm-mapping enable
[SwitchB-Vlan-interface200] quit
```

On Switch B, configure an IGMP SSM mapping for the multicast source (Source 2) and multicast groups in the range of 232.1.1.0/24.

```
[SwitchB] igmp
[SwitchB-igmp] ssm-mapping 232.1.1.0 24 10.110.5.101
[SwitchB-igmp] quit
```

Verifying the configuration

1. Send IGMPv2 reports from Host A and Host C to join the multicast group **232.1.1.1**. (Details not shown.)
2. Display multicast information on Switch A:

Display the IGMP SSM mapping information of the multicast group 232.1.1.1.

```
[SwitchA] display igmp ssm-mapping 232.1.1.1
```

```
VPN-Instance: public net
```

```
Group: 232.1.1.1
```

```
Source list:
```

```
10.110.5.100
```

Display information about the multicast group created based on the configured IGMP SSM mapping.

```
[SwitchA] display igmp ssm-mapping group
```

```
Total 1 IGMP SSM-mapping Group(s).
```

```
Interface group report information of VPN-Instance: public net
```

```
Vlan-interface100(10.110.1.1):
```

```
Total 1 IGMP SSM-mapping Group reported
```

Group	Address	Last Reporter	Uptime	Expires
232.1.1.1		10.110.1.2	00:02:04	off

Display the PIM routing table.

```
[SwitchA] display pim routing-table
```

```
VPN-Instance: public net
```

```
Total 1 (S, G) entry
```

```
(10.110.5.100, 232.1.1.1)
```

```
Protocol: pim-ssm, Flag:
```

```
UpTime: 00:13:25
```

```
Upstream interface: Vlan-interface101
```

```
Upstream neighbor: 192.168.1.2
```

```
RPF prime neighbor: 192.168.1.2
```

```
Downstream interface(s) information:
```

```
Total number of downstreams: 1
```

```
1: Vlan-interface100
```

```
Protocol: igmp, UpTime: 00:13:25, Expires: -
```

3. Display multicast information on Switch B:

Display the IGMP SSM mapping information of the multicast group 232.1.1.1.

```
[SwitchB] display igmp ssm-mapping 232.1.1.1
```

```
VPN-Instance: public net
```

```
Group: 232.1.1.1
```

```
Source list:
```

```
10.110.5.101
```

Display information about the multicast group created based on the configured IGMP SSM mapping.

```
[SwitchB] display igmp ssm-mapping group
Total 1 IGMP SSM-mapping Group(s).
Interface group report information of VPN-Instance: public net
Vlan-interface200(10.110.2.1):
```

```
Total 1 IGMP SSM-mapping Group reported
```

Group Address	Last Reporter	Uptime	Expires
232.1.1.1	10.110.2.2	00:01:15	off

Display the PIM routing table.

```
[SwitchB] display pim routing-table
VPN-Instance: public net
Total 1 (S, G) entry
```

```
(10.110.5.101, 232.1.1.1)
```

```
Protocol: pim-ssm, Flag:
```

```
UpTime: 00:12:16
```

```
Upstream interface: Vlan-interface102
```

```
Upstream neighbor: 192.168.2.2
```

```
RPF prime neighbor: 192.168.2.2
```

```
Downstream interface(s) information:
```

```
Total number of downstreams: 1
```

```
1: Vlan-interface200
```

```
Protocol: igmp, UpTime: 00:05:21, Expires: -
```

The output shows that:

- After an IGMP SSM mapping is configured on Switch A, Switch A translates (0.0.0.0, 232.1.1.1) into (10.110.5.100, 232.1.1.1). Host A can receive multicast data only from Source 1.
- After an IGMP SSM mapping is configured on Switch B, Switch B translates (0.0.0.0, 232.1.1.1) into (10.110.1.101, 232.1.1.1). Host C can receive multicast data only from Source 2.

Configuration files

- Switch A:

```
#
multicast routing-enable
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 10.110.1.1 255.255.255.0
 igmp enable
 igmp version 3
 igmp ssm-mapping enable
 pim sm
#
```

```

interface Vlan-interface101
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
#
igmp
 ssm-mapping 232.1.1.0 24 10.110.5.100
#
pim
 ssm-policy 2000
#

```

- Switch B:

```

#
multicast routing-enable
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
vlan 102
#
vlan 200
#
interface Vlan-interface102
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface Vlan-interface200
 ip address 10.110.2.1 255.255.255.0
 igmp enable
 igmp version 3
 igmp ssm-mapping enable
 pim sm
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
igmp
 ssm-mapping 232.1.1.0 24 10.110.5.101
#
pim
 ssm-policy 2000
#

```

- Switch C:


```
#
multicast routing-enable
#
acl number 2000
  rule 0 permit source 232.1.1.0 0.0.0.255
#
vlan 101 to 102
#
vlan 300
#
interface Vlan-interface101
  ip address 192.168.1.2 255.255.255.0
  pim sm
#
interface Vlan-interface102
  ip address 192.168.2.2 255.255.255.0
  pim sm
#
interface Vlan-interface300
  ip address 10.110.5.1 255.255.255.0
  pim sm
#
ospf 1
  area 0.0.0.0
    network 10.110.5.0 0.0.0.255
    network 192.168.1.0 0.0.0.255
    network 192.168.2.0 0.0.0.255
#
pim
  ssm-policy 2000
#
```

Example: Configuring IGMP proxying

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

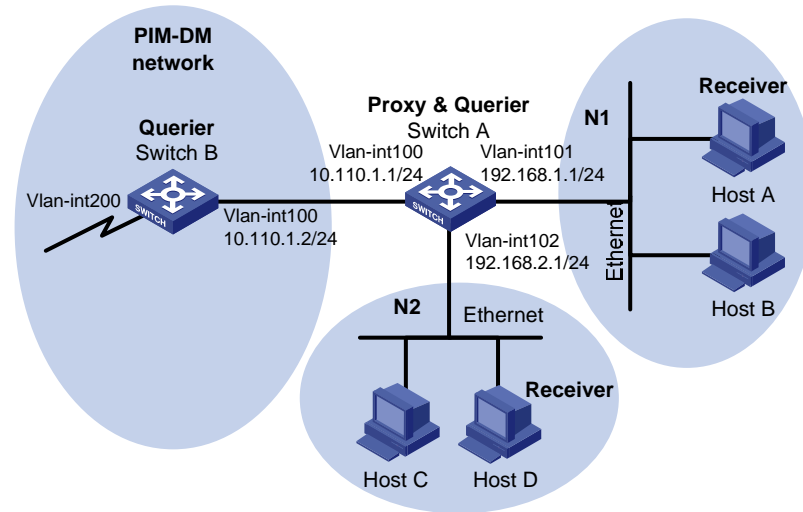
Network requirements

As shown in [Figure 76](#):

- User networks N1 and N2 connect to the IGMP querier (Switch B) in the PIM-DM domain through a Layer 3 switch (Switch A).
- All switches run OSPF, and they can communicate with each other through unicast routes.

Configure IGMP proxying on Switch A, so that the receiver hosts in N1 and N2 can receive multicast data from the PIM-DM domain even though Switch A is not running PIM-DM.

Figure 76 Network diagram



Requirements analysis

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

- Enable IGMP proxying on the upstream interface of Switch A.
- Enable IGMP on the downstream interface of Switch A.

Configuration restrictions and guidelines

When you configure IGMP proxying, follow these restrictions and guidelines:

- Enable IP multicast routing before you enable IGMP proxying.
- Only one interface of a device can be enabled with IGMP proxying.
- Do not configure IGMPv1 on the downstream interface of the IGMP proxy device. In IGMPv1, only the DR elected by PIM can serve as the IGMP querier. However, an IGMP proxy device cannot be enabled with PIM. Therefore, an IGMP proxy device cannot be elected as a DR and cannot act as an IGMP querier.

Configuration procedures

1. Assign an IP address and subnet mask to each interface, as shown in [Figure 76](#). (Details not shown.)

2. Configure Switch A:

```
# Enable IP multicast routing on Switch A.
<SwitchA> system-view
[SwitchA] multicast routing-enable

# Enable IGMP proxying on VLAN-interface 100.
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp proxying enable
[SwitchA-Vlan-interface100] quit

# Enable IGMP on VLAN-interface 101 and VLAN-interface 102.
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] igmp enable
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] igmp enable
[SwitchA-Vlan-interface102] quit
```

3. Configure Switch B:

```
# Enable IP multicast routing globally.
<SwitchB> system-view
[SwitchB] multicast routing-enable

# Enable PIM-DM on each interface.
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] pim dm
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] pim dm
[SwitchB-Vlan-interface200] quit

# Enable IGMP on VLAN-interface 100.
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] igmp enable
[SwitchB-Vlan-interface100] quit
```

Verifying the configuration

1. Send an IGMP report from Host A in N1 to join the multicast group **224.1.1.1**. (Details not shown.)
2. Display IGMP group information on Switch A and Switch B:

```
# Display IGMP group information on VLAN-interface 101 of Switch A.
[SwitchA] display igmp group interface vlan-interface 101
Vlan-interface101(192.168.1.1):
```

```

Total 1 IGMP Group reported
  Group Address   Last Reporter   Uptime         Expires
  224.1.1.1      192.168.1.10   00:10:14      00:01:10

```

The output shows that Switch A creates and maintains group membership for multicast group 224.1.1.1 after it receives the report on VLAN-interface 101. Switch A acts as an IGMP router from the perspective of downstream hosts.

Display IGMP group information on VLAN-interface 100 of Switch B.

```

[SwitchB] display igmp group interface Vlan-interface 100
Vlan-interface100(10.110.1.2):
  Total 1 IGMP Group reported
    Group Address   Last Reporter   Uptime         Expires
    224.1.1.1      10.110.1.1     00:11:14      00:01:58

```

The output shows that Switch B creates and maintains group membership for multicast group 224.1.1.1 after it receives the report from Switch A on VLAN-interface 100. Switch A acts as a receiver host from the perspective of Switch B.

Configuration files

- Switch A:


```

#
multicast routing-enable
#
vlan 100 to 102
#
interface Vlan-interface100
  igmp enable
#
interface Vlan-interface101
  igmp enable
#
interface Vlan-interface102
  igmp proxying enable
#

```
- Switch B:


```

#
multicast routing-enable
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
  igmp enable
  pim dm
#

```

```
interface Vlan-interface200
  pim dm
#
```

IGMP snooping configuration example

This chapter provides examples for configuring IGMP snooping to manage and control multicast group forwarding at Layer 2.

General configuration restrictions and guidelines

Do not enable IGMP snooping on a VLAN if the VLAN interface is running a Layer 3 multicast protocol.

Example: Configuring an IGMP snooping multicast group filter

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

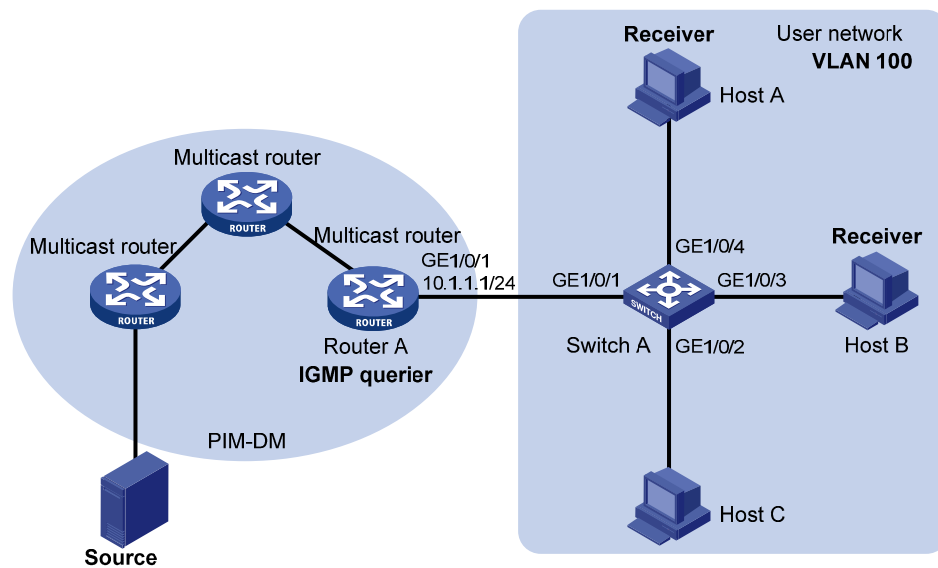
Network requirements

As shown in [Figure 77](#):

- The user network VLAN 100 is connected to the IGMP querier (Router A) in the PIM-DM domain through Switch A.
- Users in VLAN 100 want to receive multicast packets from the Source.

Configure an IGMP snooping multicast group filter on Switch A, so the receiver hosts in VLAN 100 can receive only the multicast data destined for multicast group 224.1.1.1.

Figure 77 Network diagram



Requirements analysis

To prevent the receiver hosts in VLAN 100 from receiving multicast packets for other multicast groups, enable dropping unknown multicast packets for VLAN 100.

To configure a multicast group filter, 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 if 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 GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchA] vlan 100  
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Enable IGMP snooping for VLAN 100.

```
[SwitchA-vlan100] igmp-snooping enable
```

Enable dropping unknown multicast data for VLAN 100.

```
[SwitchA-vlan100] igmp-snooping drop-unknown
[SwitchA-vlan100] quit

# Create a basic ACL for multicast group filtering.
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 224.1.1.1 0
[SwitchA-acl-basic-2001] quit

# Configure a multicast group filter that references ACL 2001 for VLAN 100.
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] group-policy 2001 vlan 100
[SwitchA-igmp-snooping] quit
```

Verifying the configuration

1. 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.)
2. Display detailed IGMP snooping group information on Switch A.

```
[SwitchA] display igmp-snooping group verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port(s).
      GE1/0/1                (D)
IP group(s):the following ip group(s) match to one mac group.
IP group address:224.1.1.1
(0.0.0.0, 224.1.1.1):
Attribute:   Host Port
Host port(s):total 1 port(s).
      GE1/0/4                (D)
MAC group(s):
MAC group address:0100-5e01-0101
Host port(s):total 1 port(s).
      GE1/0/4
```

The output shows that only information about the (0.0.0.0, 224.1.1.1) entry is displayed on Switch A. The configured multicast group filter has taken effect.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
acl number 2001
  rule 0 permit source 224.1.1.1 0
#
igmp-snooping
  group-policy 2001 vlan 100
#
vlan 100
  igmp-snooping enable
  igmp-snooping drop-unknown
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port access vlan 100
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 100
#
interface GigabitEthernet1/0/3
  port link-mode bridge
  port access vlan 100
#
interface GigabitEthernet1/0/4
  port link-mode bridge
  port access vlan 100
#
```

Example: Configuring IGMP snooping static ports

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

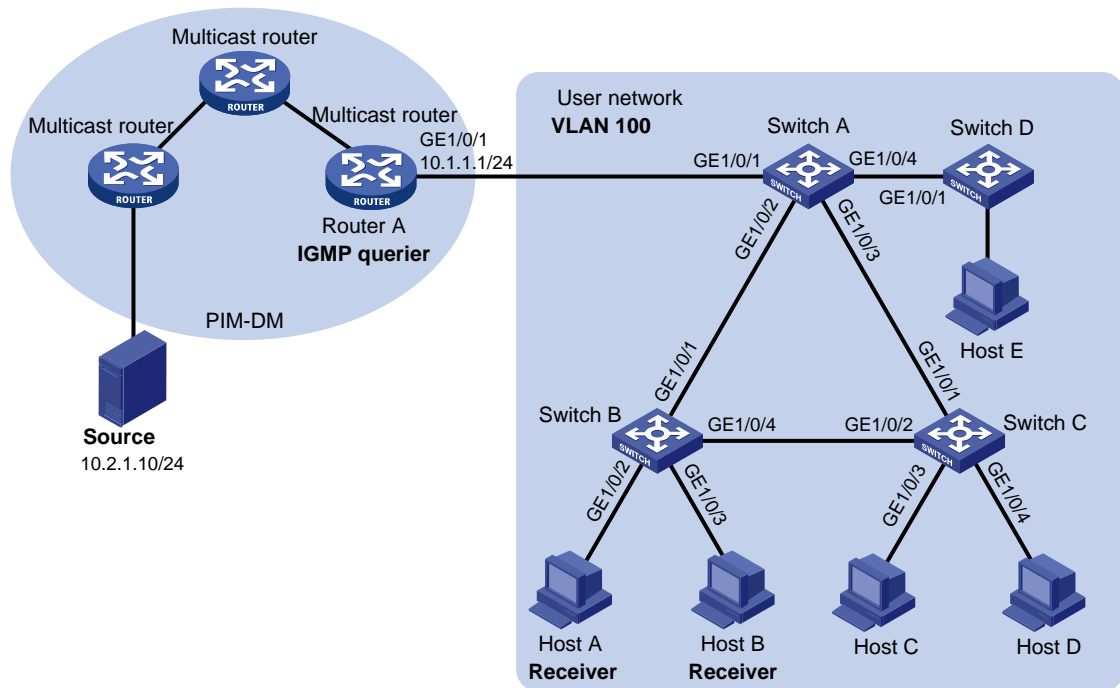
As shown in [Figure 78](#):

- The user network VLAN 100 is connected to the IGMP querier (Router A) in the PIM-DM domain through Switch A. Users in VLAN 100 want to receive multicast packets from the Source.
- In the user network, Switch A, Switch B, and Switch C form a ring and are running STP to avoid loops.
- In the user network, dropping unknown multicast packets is enabled on all switches to prevent unknown multicast packets from being flooded.

Configure IGMP snooping static member ports and static router ports to achieve the following goals:

- Host A and Host B receive only multicast packets destined for the multicast group 224.1.1.1.
- Multicast packets can switch from one failed path between Switch A and Switch B to the other path immediately after the new path comes up and becomes stable.

Figure 78 Network diagram



Requirements analysis

To make sure the receiver hosts receive multicast data for a fixed multicast group, configure the ports that are connected to the hosts as IGMP snooping static member ports.

After an STP switchover occurs and the new path becomes stable, at least one IGMP query/response exchange is required before the new path can forward multicast data. To implement an immediate switchover to the new path, configure all ports that might become the outgoing 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 GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN.
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4

# Enable IGMP snooping for VLAN 100.
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit

# Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as IGMP snooping static router ports.
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] igmp-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

Configuring Switch B

```
# Enable IGMP snooping globally.
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit

# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN.
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4

# Enable IGMP snooping for VLAN 100.
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit

# Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as static member ports for the multicast group 224.1.1.1.
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchB-GigabitEthernet1/0/3] quit
```

Configuring Switch C

```
# Enable IGMP snooping globally.
```

```

<SwitchC> system-view
[SwitchC] igmp-snooping
[SwitchC-igmp-snooping] quit

# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN.
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4

# Enable IGMP snooping for VLAN 100.
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] quit

# Configure GigabitEthernet 1/0/2 as an IGMP snooping static router port.
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] igmp-snooping static-router-port vlan 100
[SwitchC-GigabitEthernet1/0/2] quit

```

Verifying the configuration

1. Send IGMP reports from Host A and Host B to join the multicast group **224.1.1.1**. (Details not shown.)
2. Display IGMP snooping group information.

Display detailed IGMP snooping group information for VLAN 100 on Switch A.

```

[SwitchA] display igmp-snooping group vlan 100 verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 3 port.
GE1/0/1 (D)
GE1/0/2 (S)
GE1/0/3 (S)
IP group(s):the following ip group(s) match to one mac group.
IP group address:224.1.1.1
(0.0.0.0, 224.1.1.1):
Attribute: Host Port
Host port(s):total 1 port.
GE1/0/2 (D)
MAC group(s):
MAC group address:0100-5e01-0101
Host port(s):total 1 port.
GE1/0/2

```

The output shows that GigabitEthernet 1/0/2 and GigabitEthernet1/0/3 on Switch A have become IGMP snooping static router ports.

Display detailed IGMP snooping group information for VLAN 100 on Switch B.

```
[SwitchB] display igmp-snooping group vlan 100 verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port.
    GE1/0/2                (D)
IP group(s):the following ip group(s) match to one mac group.
    IP group address:224.1.1.1
    (0.0.0.0, 224.1.1.1):
        Attribute:      Host Port
    Host port(s):total 2 port.
        GE1/0/2                (S)
        GE1/0/3                (S)
MAC group(s):
    MAC group address:0100-5e01-0101
    Host port(s):total 2 port.
        GE1/0/2
        GE1/0/3
```

The output shows that GigabitEthernet1/0/2 and GigabitEthernet 1/0/3 on Switch B have become the static member ports for multicast group 224.1.1.1.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```
#
igmp-snooping
#
vlan 100
igmp-snooping enable
#
interface GigabitEthernet1/0/1
port link-mode bridge
port access vlan 100
#
interface GigabitEthernet1/0/2
```

```

port link-mode bridge
port access vlan 100
igmp-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/3
port link-mode bridge
port access vlan 100
igmp-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/4
port link-mode bridge
port access vlan 100
#

```

- **Switch B:**

```

#
igmp-snooping
#
vlan 100
igmp-snooping enable
#
interface GigabitEthernet1/0/1
port link-mode bridge
port access vlan 100
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 100
igmp-snooping static group 224.1.1.1 vlan 100
#
interface GigabitEthernet1/0/3
port link-mode bridge
port access vlan 100
igmp-snooping static-group 224.1.1.1 vlan 100
#
interface GigabitEthernet1/0/4
port link-mode bridge
port access vlan 100
#

```

- **Switch C:**

```

#
igmp-snooping
#
vlan 100
igmp-snooping enable
#
interface GigabitEthernet1/0/1
port link-mode bridge
port access vlan 100

```

```
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 100
  igmp-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/3
  port link-mode bridge
  port access vlan 100
#
interface GigabitEthernet1/0/4
  port link-mode bridge
  port access vlan 100
#
```

Example: Configuring an IGMP snooping querier

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

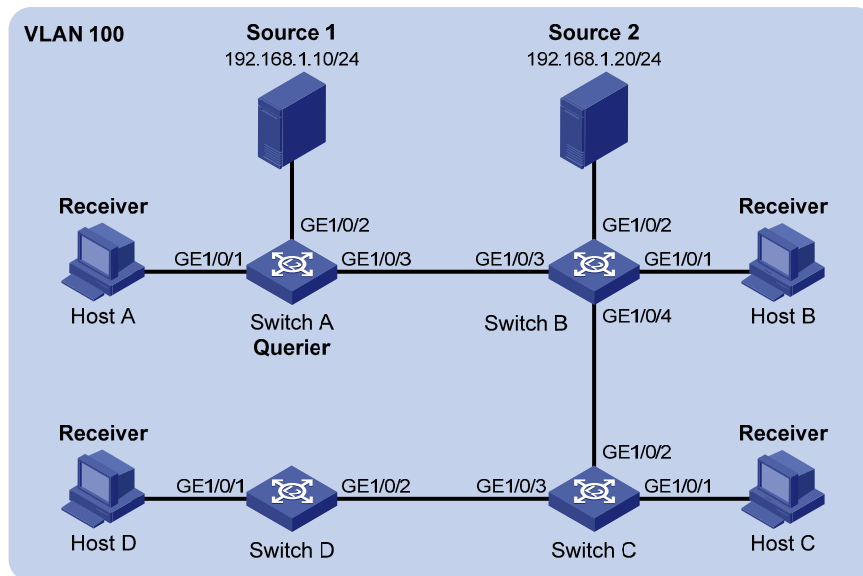
Network requirements

As shown in [Figure 79](#):

- The network is a Layer 2-only network.
- Source 1 and Source 2 send multicast data to the multicast groups 224.1.1.1 and 225.1.1.1, respectively.
- Host A and Host C are receivers of multicast group 224.1.1.1, and Host B and Host D are receivers of multicast group 225.1.1.1.

Configure an IGMP snooping querier so the receiver hosts can receive their expected multicast packets.

Figure 79 Network diagram



Requirements analysis

To establish and maintain Layer 2 multicast forwarding entries, configure the switch that is close to the multicast source (Switch A in this example) as the IGMP snooping querier.

After a switch receives an IGMP query with the source IP address of 0.0.0.0 on a port, it does not enlist the port as a dynamic router port. This might prevent multicast forwarding entries from being correctly created at the data link layer. To avoid this problem, you must configure a non-all-zero IP address as the source IP address of IGMP queries when a Layer 2 switch acts as the IGMP snooping querier.

Configuration procedures

Configuring Switch A

Enable IGMP snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to this VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

Enable IGMP snooping and IGMP snooping querier for VLAN 100.

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping querier
```

Specify the source IP address as 192.168.1.1 for the general queries and group-specific queries in VLAN 100.

```
[SwitchA-vlan100] igmp-snooping general-query source-ip 192.168.1.1
[SwitchA-vlan100] igmp-snooping special-query source-ip 192.168.1.1
[SwitchA-vlan100] quit
```

Configuring Switch B

Enable IGMP snooping globally.

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

Create VLAN 100, and assign GigabitEthernet1/0/1 through GigabitEthernet1/0/4 to this VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Enable IGMP snooping for VLAN 100.

```
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

Configuring Switch C and Switch D

Configure Switch C and Switch D in the same way Switch B is configured. (Details not shown.)

Verifying the configuration

Display statistics for IGMP packets that have been received on Switch B.

```
[SwitchB-vlan100] display igmp-snooping statistics
Received IGMP general queries:96.
Received IGMPv1 reports:0.
Received IGMPv2 reports:105.
Received IGMP leaves:0.
Received IGMPv2 specific queries:0.
Sent IGMPv2 specific queries:0.
Received IGMPv3 reports:0.
Received IGMPv3 reports with right and wrong records:0.
Received IGMPv3 specific queries:0.
Received IGMPv3 specific sg queries:0.
Sent IGMPv3 specific queries:0.
Sent IGMPv3 specific sg queries:0.
Received error IGMP messages:0.
```

The output shows that the configured IGMP snooping querier has successfully sent out IGMP queries.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```
#
igmp-snooping
```

```

#
vlan 100
  igmp-snooping enable
  igmp-snooping querier
  igmp-snooping general-query source-ip 192.168.1.1
  igmp-snooping special-query source-ip 192.168.1.1
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port access vlan 100
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 100
#
interface GigabitEthernet1/0/3
  port link-mode bridge
  port access vlan 100
#

```

- Switch B:

```

#
  igmp-snooping
#
vlan 100
  igmp-snooping enable
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port access vlan 100
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 100
#
interface GigabitEthernet1/0/3
  port link-mode bridge
  port access vlan 100
#
interface GigabitEthernet1/0/4
  port link-mode bridge
  port access vlan 100
#

```

The configuration information on Switch C and Switch D is similar to that on Switch B. (Details not shown.)

Example: Configuring IGMP snooping proxying

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

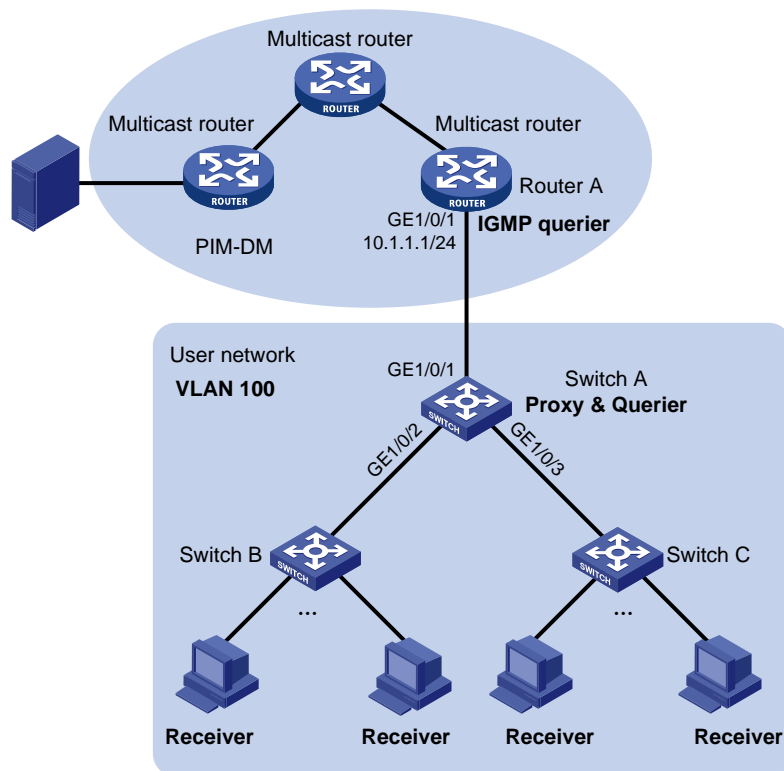
Network requirements

As shown in [Figure 80](#):

- The user network VLAN 100 is connected to the IGMP querier (Router A) in the PIM-DM domain through Switch A.
- IGMP snooping is enabled on all switches in VLAN 100.
- Many receivers in VLAN 100 require different VOD data. The receivers frequently join or leave multicast groups, sending large amount of IGMP report and leave messages to the IGMP querier.

Configure an IGMP snooping proxy to reduce the burden on the IGMP querier.

Figure 80 Network diagram



Requirements analysis

To reduce the number of IGMP report and leave messages received by upstream devices, enable IGMP snooping proxying on the device that is close to the IGMP querier (Switch A in this example).

Configuration restrictions and guidelines

Before configuring IGMP snooping proxying, enable IGMP snooping globally and for the relevant VLANs.

Configuration procedures

Configuring Switch A

```
# Enable IGMP snooping globally.
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit

# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to this VLAN.
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3

# Enable IGMP snooping and IGMP snooping proxying for VLAN 100.
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping proxying enable

# Configure the source IP address for IGMP report and leave messages sent by the proxy.
[SwitchA-vlan100] igmp-snooping report source-ip 10.1.1.100
[SwitchA-vlan100] igmp-snooping leave source-ip 10.1.1.100
[SwitchA-vlan100] quit
```

Configuring Switch B and Switch C

```
# Create VLAN 100, and assign ports that connects to the receiver hosts to the VLAN. Enable IGMP
snooping for the VLAN. (Details not shown.)
```

Verifying the configuration

1. Send IGMP reports from the receiver hosts in VLAN 100 to join the multicast group **224.1.1.1**. (Details not shown.)
2. Display IGMP group information on Router A.

```
[RouterA] display igmp group
Total 1 IGMP Group(s).
Interface group report information of VPN-Instance: public net
GigabitEthernet1/0/1(10.1.1.1):
```

```
Total 1 IGMP Group reported
```

Group Address	Last Reporter	Uptime	Expires
224.1.1.1	10.1.1.100	00:00:06	00:02:04

The output shows that the last reporter address for the multicast group 224.1.1.1 is the configured source IP address for IGMP reports sent by the proxy. Switch A has sent IGMP reports to Router A on behalf of the receiver hosts.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
 igmp-snooping
#
vlan 100
 igmp-snooping enable
 igmp-snooping proxying enable
 igmp-snooping report source-ip 10.1.1.100
 igmp-snooping leave source-ip 10.1.1.100
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
```

IP addressing configuration examples

This chapter provides IP addressing configuration examples.

Example: Configuring IP addressing

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

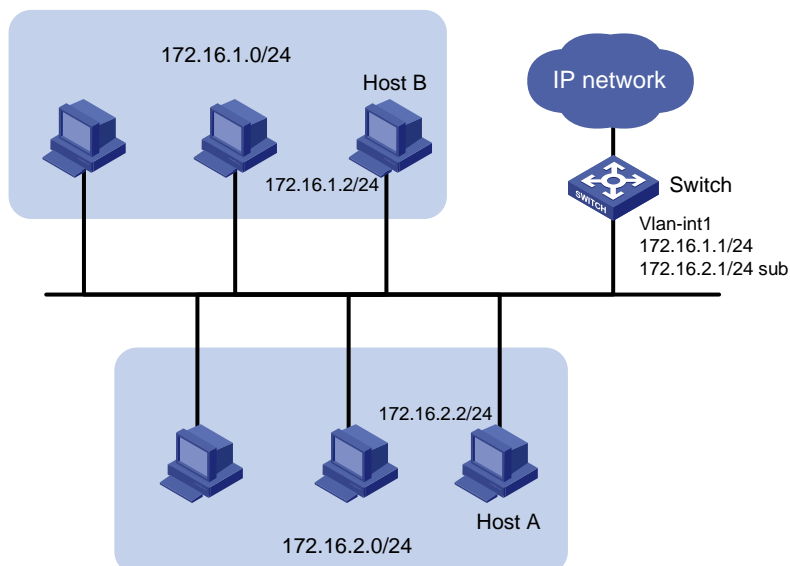
Network requirements

As shown in [Figure 81](#):

- Set the primary IP address of the switch as the gateway address of the hosts on subnet 172.16.1.0/24.
- Set the secondary IP address of the switch as the gateway address of the hosts on subnet 172.16.2.0/24.

The hosts on the LAN can communicate with the external network through the switch.

Figure 81 Network diagram



Configuration procedures

1. Configure the switch:

```

# Assign a primary IP address to VLAN-interface 1.
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 172.16.1.1 255.255.255.0
# Assign a secondary IP address to VLAN-interface 1.
[Switch-Vlan-interface1] ip address 172.16.2.1 255.255.255.0 sub
[Switch-Vlan-interface1] return

```

2. Set the 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: 56 data bytes, press CTRL_C to break
  Reply from 172.16.1.2: bytes=56 Sequence=1 ttl=255 time=25 ms
  Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=255 time=27 ms
  Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=255 time=26 ms
  Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=255 time=26 ms
  Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=255 time=26 ms

--- 172.16.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
round-trip min/avg/max = 25/26/27 ms

```

The output shows that the switch can communicate with the hosts on subnet 172.16.1.0/24.

Ping a host on subnet 172.16.2.0/24 from the switch to check the connectivity.

```

<Switch> ping 172.16.2.2
PING 172.16.2.2: 56 data bytes, press CTRL_C to break
  Reply from 172.16.2.2: bytes=56 Sequence=1 ttl=255 time=25 ms
  Reply from 172.16.2.2: bytes=56 Sequence=2 ttl=255 time=26 ms
  Reply from 172.16.2.2: bytes=56 Sequence=3 ttl=255 time=26 ms
  Reply from 172.16.2.2: bytes=56 Sequence=4 ttl=255 time=26 ms
  Reply from 172.16.2.2: bytes=56 Sequence=5 ttl=255 time=26 ms

--- 172.16.2.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
round-trip min/avg/max = 25/25/26 ms

```

The output shows that the switch can communicate with the hosts on subnet 172.16.2.0/24.

Configuration files

```
#  
interface Vlan-interface1  
  ip address 172.16.1.1 255.255.255.0  
  ip address 172.16.2.1 255.255.255.0 sub  
#
```

IP performance optimization configuration examples

This chapter provides IP performance optimization configuration examples.

Example: Enabling an interface to forward directed broadcasts destined for the directly connected network

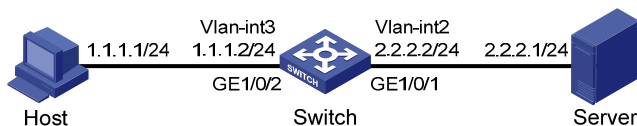
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 82](#), enable VLAN-interface 2 to forward directed broadcasts destined for the directly connected network. The server can receive directed broadcasts from the host to IP address 2.2.2.255.

Figure 82 Network diagram



Configuration procedures

1. Configure the switch:

```
# Create VLAN 2, and assign GigabitEthernet 1/0/1 to VLAN 2.
```

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] port GigabitEthernet 1/0/1
[Switch-Vlan2] quit
```

```

# Create VLAN 3, and assign GigabitEthernet 1/0/2 to VLAN 3.
[Switch] Vlan 3
[Switch-vlan3] port GigabitEthernet 1/0/2
[Switch-Vlan3] quit

# Specify IP addresses for VLAN-interface 3 and VLAN-interface 2.
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 1.1.1.2 24
[Switch-Vlan-interface3] quit
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 2.2.2.2 24

# Enable VLAN-interface 2 to forward directed broadcasts destined for the directly connected
network.
[Switch-Vlan-interface2] ip forward-broadcast

```

2. Specify the IP address of VLAN-interface 3 as the gateway address of the host.

Verifying the configuration

Ping the subnet-directed broadcast address 2.2.2.255 on the host. The server can receive the ping packets.

Execute the **undo ip forward-broadcast** command on VLAN-interface 2. The server cannot receive the ping packets.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```

#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 2.2.2.2 255.255.255.0
 ip forward-broadcast
#
interface Vlan-interface3
 ip address 1.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#

```


Example: Enabling a device to send ICMP destination unreachable packets

When a device is enabled to send ICMP destination unreachable packets, it does the following:

- Discards a packet when it cannot route or deliver the packet.
- Sends an ICMP destination unreachable packet to the source.

Applicable product matrix

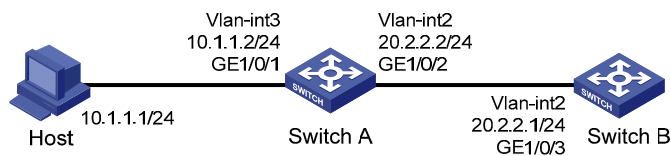
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 83](#), specify Switch A as the default gateway of the host.

Enable Switch A to send ICMP destination unreachable packets to the host when the IP address of Switch B is incorrectly entered on the host.

Figure 83 Network Diagram



Configuration procedures

1. Configure Switch A:

```
# Enable sending ICMP destination unreachable packets.
<SwitchA> system-view
[SwitchA] ip unreachable enable

# Create VLAN 3, and assign GigabitEthernet 1/0/1 to VLAN 3.
[SwitchA] vlan 3
[SwitchA-vlan3] port GigabitEthernet 1/0/1
[SwitchA-Vlan3] quit

# Create VLAN 2, and assign GigabitEthernet 1/0/2 to VLAN 2.
[SwitchA] vlan 2
```

```
[SwitchA-vlan2] port GigabitEthernet 1/0/2
[SwitchA-Vlan2] quit
# Specify IP addresses for VLAN-interface 3 and VLAN-interface 2.
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 10.1.1.2 24
[SwitchA-Vlan-interface3] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 20.2.2.2 24
```

2. Configure Switch B:

Create VLAN 2, and assign GigabitEthernet 1/0/3 to VLAN 2.

```
<SwitchB> system-view
[SwitchB] Vlan 2
[SwitchB-vlan2] port GigabitEthernet 1/0/3
[SwitchB-Vlan2] quit
# Specify the IP address for VLAN-interface 2.
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 20.2.2.1 24
# Configure a static route for Switch B to the host.
[SwitchB] ip route-static 10.1.1.0 24 20.2.2.2
```

3. Specify the IP address of VLAN-interface 3 of the switch as the gateway address of the host.

Verifying the configuration

Ping 20.2.2.1 from the host to check the connectivity.

```
C:\ping 20.2.2.1
```

```
Pinging 20.2.2.1 with 32 bytes of data:
```

```
Reply from 20.2.2.1: bytes=32 time=6ms TTL=254
Reply from 20.2.2.1: bytes=32 time=1ms TTL=254
Reply from 20.2.2.1: bytes=32 time=1ms TTL=254
Reply from 20.2.2.1: bytes=32 time=1ms TTL=254
```

```
Ping statistics for 20.2.2.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 6ms, Average = 2ms
```

Ping 30.2.2.1 from the host to check the connectivity.

```
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

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```
#
 ip unreachable enable
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 20.2.2.2 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
 ip route-static 10.1.1.0 255.255.255.0 20.2.2.2
#
```

- Switch B:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 20.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode bridge
```

```
port access vlan 2
#
ip route-static 10.1.1.0 255.255.255.0 20.2.2.2
```

IP source guard configuration examples

This chapter provides IP source guard configuration examples.

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 5500 EI	Release 2220
HP 5500 SI	

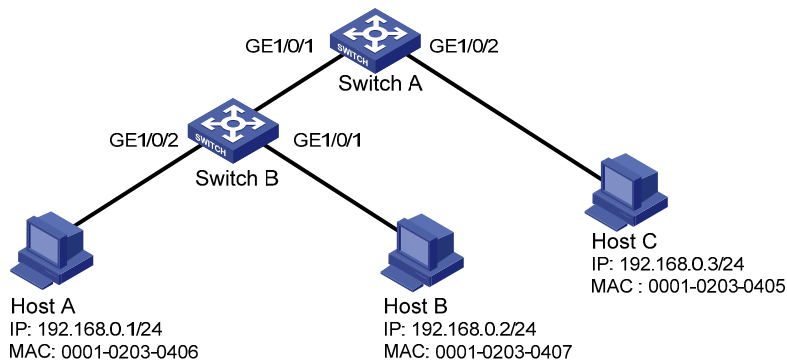
Network requirements

As shown in [Figure 84](#), Host A, B, and C use static IP addresses.

Configure static IPv4 source guard binding entries on Switch A and Switch B to meet the following requirements:

- GigabitEthernet 1/0/1 on Switch A allows only IP packets from Host A to pass.
- GigabitEthernet 1/0/2 on Switch A and interfaces on Switch B allow only IP packets from their own directly connected hosts to pass.

Figure 84 Network diagram



Configuration procedures

1. Configure Switch A:

Enable IPv4 source guard on GigabitEthernet 1/0/2 to filter incoming packets by checking their source IPv4 addresses and source MAC addresses.

```
<SwitchA> system-view
```

```
[SwitchA] interface gigabitethernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

Bind IP address 192.168.0.3 with MAC address 0001-0203-0405 to form a static IP source guard binding entry on GigabitEthernet 1/0/2.

```
[SwitchA-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.3 mac-address 0001-0203-0405
```

```
[SwitchA-GigabitEthernet1/0/2] quit
```

Enable IPv4 source guard on GigabitEthernet 1/0/1 to filter incoming packets by checking their source IPv4 addresses and source MAC addresses.

```
[SwitchA] interface gigabitethernet 1/0/1
```

```
[SwitchA-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

Bind IP address 192.168.0.1 with MAC address 0001-0203-0406 to form a static IP source guard binding entry on GigabitEthernet 1/0/1.

```
[SwitchA-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
```

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

2. Configure Switch B:

Enable IPv4 source guard on GigabitEthernet 1/0/2 to filter incoming packets by checking their source IPv4 addresses and source MAC addresses.

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

```
[SwitchB] interface gigabitethernet 1/0/2
```

```
[SwitchB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

Bind IP address 192.168.0.1 with MAC address 0001-0203-0406 to form a static IP source guard entry on GigabitEthernet 1/0/2.

```
[SwitchB-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.1 mac-address
0001-0203-0406
[SwitchB-GigabitEthernet1/0/2] quit
# Enable IPv4 source guard on GigabitEthernet 1/0/1 to filter incoming packets by checking their
source IPv4 addresses and source MAC addresses.
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-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 GigabitEthernet 1/0/1.
[SwitchB-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.2 mac-address
0001-0203-0407
[SwitchB-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display IPv4 source guard binding entries on Switch A.

```
[SwitchA] display ip source binding static
Total entries found: 2
```

MAC Address	IP Address	VLAN	Interface	Type
0001-0203-0406	192.168.0.1	N/A	GE1/0/1	Static
0001-0203-0405	192.168.0.3	N/A	GE1/0/2	Static

Display IPv4 source guard binding entries on Switch B.

```
[SwitchB] display ip source binding static
Total entries found: 2
```

MAC Address	IP Address	VLAN	Interface	Type
0001-0203-0407	192.168.0.2	N/A	GE1/0/1	Static
0001-0203-0406	192.168.0.1	N/A	GE1/0/2	Static

Configuration files

- Switch A:

```
#
interface GigabitEthernet1/0/1
 ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
 ip verify source ip-address mac-address
#
interface GigabitEthernet1/0/2
 ip source binding ip-address 192.168.0.3 mac-address 0001-0203-0405
 ip verify source ip-address mac-address
#
```
- Switch B:

```
#
interface GigabitEthernet1/0/1
 ip source binding ip-address 192.168.0.2 mac-address 0001-0203-0407
```

```
ip verify source ip-address mac-address
#
interface GigabitEthernet1/0/2
ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
ip verify source ip-address mac-address
#
```

Example: Configuring static and dynamic IP source guard binding entries

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

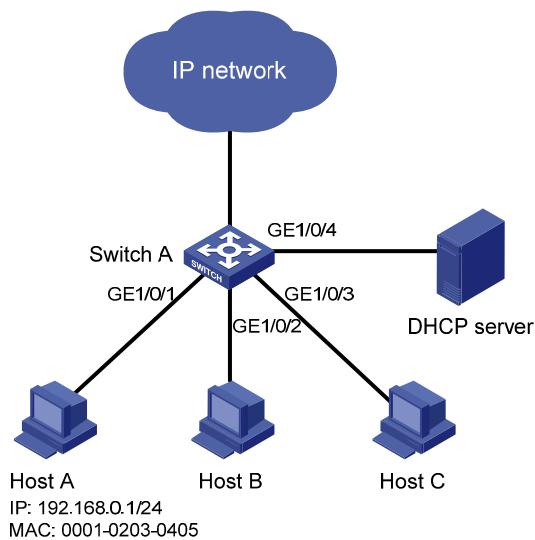
As shown in [Figure 85](#):

- 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:

- GigabitEthernet 1/0/1 on Switch A allows only packets from Host A to pass.
- GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 on Switch A allow only packets from Host B and Host C to pass.

Figure 85 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 GigabitEthernet 1/0/1 of Switch A.
- To allow packets from Host B and Host C to access the network, configure IP source guard on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3. IP source guard check 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 GigabitEthernet 1/0/1 to filter incoming packets by checking their source IPv4 addresses and source MAC addresses.

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

Bind IP address 192.168.0.1 with MAC address 0001-0203-0405 to form a static IPv4 source guard binding entry on GigabitEthernet 1/0/1.

```
[SwitchA-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0203-0405
```

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

# Specify GigabitEthernet 1/0/4 as a trusted port.
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] dhcp-snooping trust
[SwitchA-GigabitEthernet1/0/4] quit

# Enable DHCP snooping.
[SwitchA] dhcp-snooping

# Enable IPv4 source guard on GigabitEthernet 1/0/2 to filter incoming packets by checking their
source IPv4 addresses and source MAC addresses.
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] ip verify source ip-address mac-address
[SwitchA-GigabitEthernet1/0/2] quit

# Enable IPv4 source guard on GigabitEthernet 1/0/3 to filter incoming packets by checking their
source IPv4 addresses and source MAC addresses.
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] ip verify source ip-address mac-address
[SwitchA-GigabitEthernet1/0/3] quit
```

Verifying the configuration

Display IPv4 source guard binding entries.

```
<SwitchA> display ip source binding
Total entries found: 3
  MAC Address      IP Address      VLAN   Interface      Type
  0001-0203-0405   192.168.0.1    N/A    GE1/0/1        Static
  0001-0203-0406   192.168.0.2    1      GE1/0/2        DHCP-SNP
  0001-0203-0407   192.168.0.3    1      GE1/0/3        DHCP-SNP
```

Display DHCP snooping entries.

```
<SwitchA> display dhcp-snooping
DHCP Snooping is enabled.
The client binding table for all ports.
Type : D--Dynamic , S--Static , R--Recovering
Type IP Address      MAC Address      Lease      VLAN SVLAN Interface
==== =====
D    192.168.0.2       0001-0203-0406  86335      1    N/A   GigabitEthernet1/0/2
D    192.168.0.3       0001-0203-0407  86335      1    N/A   GigabitEthernet1/0/3
```

The output shows that dynamic IP source guard obtains DHCP snooping entries.

Configuration files

```
#
dhcp-snooping
#
```

```
interface GigabitEthernet1/0/1
  ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0405
  ip verify source ip-address mac-address
#
interface GigabitEthernet1/0/2
  ip verify source ip-address mac-address
#
interface GigabitEthernet1/0/3
  ip verify source ip-address mac-address
#
interface GigabitEthernet1/0/4
  dhcp-snooping trust
#
```

IPv6 basics configuration examples

This chapter provides configuration examples for basic IPv6 settings.

Example: Configuring basic IPv6 settings

Applicable product matrix

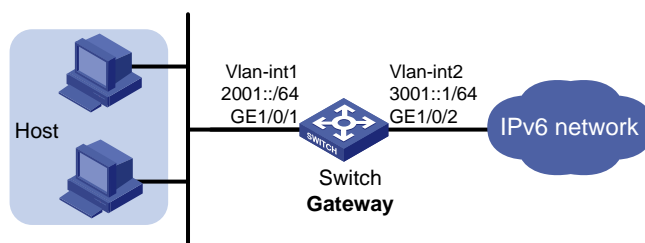
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 86](#):

- 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 86 Network diagram



Configuration procedures

1. Configure the switch:

```
# Enable IPv6.
```

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

```
[Switch] ipv6
```

```
# Specify an EUI-64 IPv6 address for VLAN-interface 1.
```

```
[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 GigabitEthernet 1/0/2  
[Switch-vlan2] quit  
[Switch] interface vlan-interface 2  
[Switch-Vlan-interface2] ipv6 address 3001::1 64  
[Switch-Vlan-interface2] quit
```

2. Configure the hosts:

Use the **cmd** command on each host to enter the DOS environment, and then enable IPv6 for the host.

```
C:\Documents and Settings\aa>ipv6 install
```

Verifying the configuration

Display the IPv6 address on a host. The output shows that the host generated an IPv6 address with the prefix 2001::/64, and the gateway is the switch.

Display the IPv6 interface settings on the switch. All the IPv6 addresses configured on the interface are displayed.

```
<Switch> display ipv6 interface  
Vlan-interfacel current state :UP  
Line protocol current state :UP  
IPv6 is enabled, link-local address is FE80::223:89FF:FE5F:958C  
Global unicast address(es):  
2001::223:89FF:FE5F:958C, subnet is 2001::/64  
Joined group address(es):  
FF02::1:FF00:0  
FF02::1:FF5F:958C  
FF02::2  
FF02::1  
MTU is 1500 bytes  
ND DAD is enabled, number of DAD attempts: 1  
ND reachable time is 30000 milliseconds  
ND retransmit interval is 1000 milliseconds  
ND advertised reachable time is 0 milliseconds  
ND advertised retransmit interval is 0 milliseconds  
ND router advertisements are sent every 600 seconds  
ND router advertisements live for 1800 seconds  
Hosts use stateless autoconfig for addresses  
IPv6 Packet statistics:  
InReceives: 67
```

```

InTooShorts:          0
InTruncatedPkts:     0
InHopLimitExceeds:   0
InBadHeaders:        0
InBadOptions:        0
ReasmReqds:          0
ReasmOKs:            0
InFragDrops:         0
InFragTimeouts:     0
OutFragFails:        0
InUnknownProtos:    0
InDelivers:          26
OutRequests:         36
OutForwDatagrams:    0
InNoRoutes:          0
InTooBigErrors:      0
OutFragOKs:          0
OutFragCreates:      0
InMcastPkts:         22
InMcastNotMembers:   41
OutMcastPkts:        21
InAddrErrors:        0
InDiscards:          0
OutDiscards:         0

```

Vlan-interface2 current state :UP

Line protocol current state :UP

IPv6 is enabled, link-local address is FE80::223:89FF:FE5F:958C

Global unicast address(es):

3001::1, subnet is 3001::/64

Joined group address(es):

FF02::1:FF00:0

FF02::1:FF00:1

FF02::1:FF5F:958C

FF02::2

FF02::1

MTU is 1500 bytes

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds

ND retransmit interval is 1000 milliseconds

Hosts use stateless autoconfig for addresses

IPv6 Packet statistics:

```

InReceives:          8
InTooShorts:         0
InTruncatedPkts:     0
InHopLimitExceeds:   0
InBadHeaders:        0
InBadOptions:        0
ReasmReqds:          0

```

```
ReasmOKs: 0
InFragDrops: 0
InFragTimeouts: 0
OutFragFails: 0
InUnknownProtos: 0
InDelivers: 6
OutRequests: 8
OutForwDatagrams: 0
InNoRoutes: 0
InTooBigErrors: 0
OutFragOKs: 0
OutFragCreates: 0
InMcastPkts: 3
InMcastNotMembers: 2
OutMcastPkts: 4
InAddrErrors: 0
InDiscards: 0
OutDiscards: 0
```

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
  ipv6
#
vlan 1 to 2
#
interface Vlan-interface1
  undo ipv6 nd ra halt
  ipv6 address 2001::/64 eui-64
#
interface Vlan-interface2
  ipv6 address 3001::1/64
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 2
#
```

IPv6 multicast VLAN configuration examples

This document provides examples for configuring IPv6 multicast VLANs to reduce the traffic load on Layer 3 devices.

IPv6 multicast VLANs include sub-VLAN-based IPv6 multicast VLANs and port-based IPv6 multicast VLANs.

- In a sub-VLAN-based IPv6 multicast VLAN, MLD snooping manages router ports in the IPv6 multicast VLAN and user ports in each sub-VLAN. It is applicable to all networking environments.
- In a port-based IPv6 multicast VLAN, MLD snooping manages both router ports and user ports in the IPv6 multicast VLAN. Port-based IPv6 multicast VLANs are typically deployed on devices that are directly connected to receivers. Port-based IPv6 multicast VLANs are easier to implement than sub-VLAN-based multicast VLANs.

General configuration restrictions and guidelines

When you configure IPv6 multicast VLANs, follow these restrictions and guidelines:

- Do not configure IPv6 multicast VLAN on a device with IPv6 multicast routing enabled.
- The port-based IPv6 multicast VLAN takes precedence over the sub-VLAN-based IPv6 multicast VLAN if they are both configured on a device.

Example: Configuring a sub-VLAN-based IPv6 multicast VLAN

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

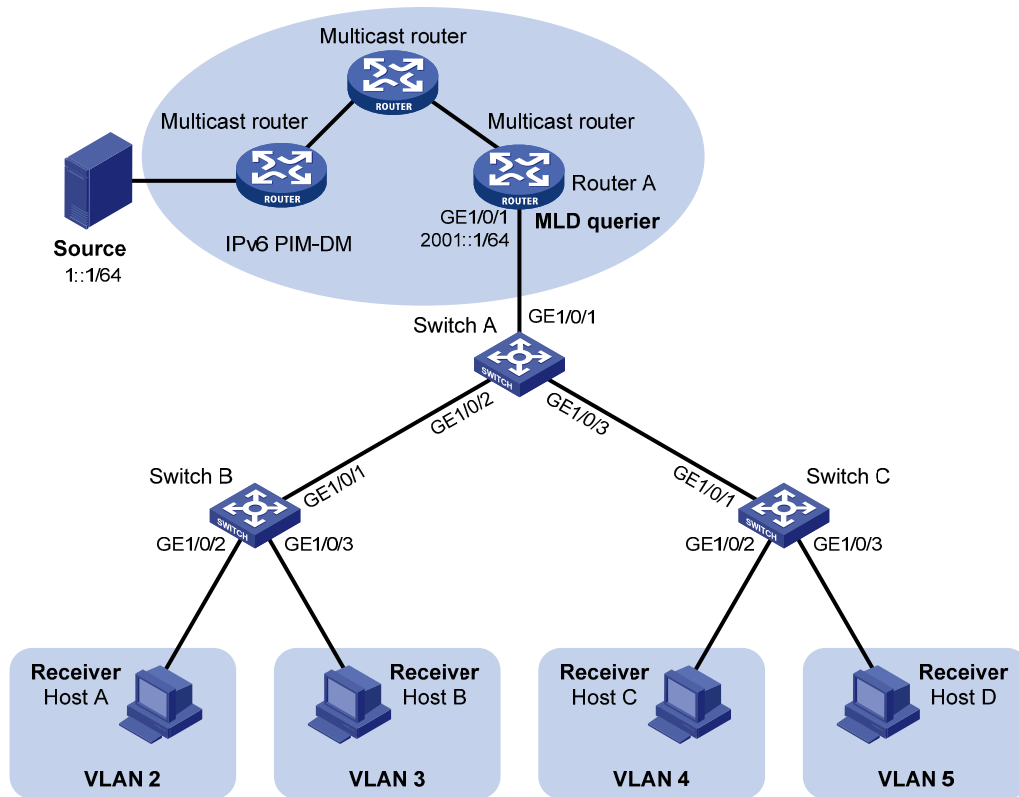
Network requirements

As shown in [Figure 87](#):

- The Layer 2 user network is connected to the MLD querier (Router A) in the IPv6 PIM-DM domain through Switch A.
- Each user VLAN has a receiver that belongs to the same IPv6 multicast group.

To save bandwidth and reduce the burden on Layer 3 multicast routers, configure a sub-VLAN-based IPv6 multicast VLAN on Switch A. In this scenario, Layer 3 multicast routers only need to forward multicast data to the multicast VLAN, and the receiver hosts in different user VLANs can receive the data.

Figure 87 Network diagram



Configuration restrictions and guidelines

When you configure a sub-VLAN-based IPv6 multicast VLAN, follow these restrictions and guidelines:

- The VLAN to be configured as the IPv6 multicast VLAN must exist.
- The VLAN to be configured as a sub-VLAN must exist and must not be an IPv6 multicast VLAN or a sub-VLAN of any other IPv6 multicast VLANs.
- After you enable the MLD snooping for the IPv6 multicast VLAN, the sub-VLANs are automatically enabled with MLD snooping.

Configuration procedures

1. Enable IPv6 forwarding on the switches. (Details not shown.)
2. Configure Switch A:

```
# Enable MLD snooping globally.
```

```
<SwitchA> system-view
```

```

[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
# Create VLAN 2 through VLAN 5. Configure GigabitEthernet 1/0/2 as a trunk port, and assign
it to VLAN 2 and VLAN 3.
[SwitchA] vlan 2 to 5
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 2 3
[SwitchA-GigabitEthernet1/0/2] quit
# Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLAN 4 and VLAN 5.
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 4 5
[SwitchA-GigabitEthernet1/0/3] quit
# Create VLAN 1024, and assign GigabitEthernet 1/0/1 to this VLAN.
[SwitchA] vlan 1024
[SwitchA-vlan1024] port gigabitethernet 1/0/1
# Enable MLD snooping for VLAN 1024.
[SwitchA-vlan1024] mld-snooping enable
[SwitchA-vlan1024] quit
# Configure VLAN 1024 as an IPv6 multicast VLAN. Configure VLAN 2 through VLAN 5 as the
sub-VLANs.
[SwitchA] multicast-vlan ipv6 1024
[SwitchA-ipv6-mvlan-1024] subvlan 2 to 5

```

3. Configure Switch B:

```

# Enable MLD snooping globally.
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
# Create VLAN 2, and assign GigabitEthernet 1/0/2 to this VLAN.
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/2
# Enable MLD snooping for VLAN 2.
[SwitchB-vlan2] mld-snooping enable
[SwitchB-vlan2] quit
# Configure VLAN 3, and assign GigabitEthernet 1/0/3 to the VLAN. Enable MLD snooping for
the VLAN. (Details not shown.)
# Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLAN 2 and VLAN 3.
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2 3

```

4. Configure Switch C in the same way Switch B is configured. (Details not shown.)

Verifying the configuration

1. Send MLD reports from the receiver hosts in the user VLANs to join the IPv6 multicast group **FF1E::101**. (Details not shown.)
2. Verify that Switch A can receive the reports and forwards the reports to Router A.

Display information about the IPv6 multicast VLAN and its sub-VLANs.

```
[SwitchA] display multicast-vlan ipv6
Total 1 IPv6 multicast-vlan(s)
```

```
IPv6 multicast vlan 1024
```

```
subvlan list:
```

```
vlan 2-5
```

```
port list:
```

```
no port
```

Display MLD snooping group information on Switch A.

```
[SwitchA] display mld-snooping group
```

```
Total 5 IP Group(s).
```

```
Total 5 IP Source(s).
```

```
Total 5 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
```

```
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
Vlan(id):2.
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Router port(s):total 0 port.
```

```
IP group(s):the following ip group(s) match to one mac group.
```

```
IP group address: FF1E::101
```

```
(::,FF1E::101):
```

```
Host port(s):total 1 port.
```

```
GE1/0/2 (D)
```

```
MAC group(s):
```

```
MAC group address:3333-0000-0101
```

```
Host port(s):total 1 port.
```

```
GE1/0/2
```

```
Vlan(id):3.
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Router port(s):total 0 port.
```

```
IP group(s):the following ip group(s) match to one mac group.
```

```
IP group address: FF1E::101
```

```
(::, FF1E::101):
```

```
Host port(s):total 1 port.
```

```
GE1/0/2 (D)
MAC group(s):
  MAC group address:3333-0000-0101
  Host port(s):total 1 port.
  GE1/0/2
```

Vlan(id):4.

```
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
```

Router port(s):total 0 port.

IP group(s):the following ip group(s) match to one mac group.

```
IP group address: FF1E::101
( :, FF1E::101):
```

Host port(s):total 1 port.

```
GE1/0/3 (D)
```

```
MAC group(s):
  MAC group address:3333-0000-0101
  Host port(s):total 1 port.
  GE1/0/3
```

Vlan(id):5.

```
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
```

Router port(s):total 0 port.

IP group(s):the following ip group(s) match to one mac group.

```
IP group address: FF1E::101
( :, FF1E::101):
```

Host port(s):total 1 port.

```
GE1/0/3 (D)
```

```
MAC group(s):
  MAC group address: 3333-0000-0101
  Host port(s):total 1 port.
  GE1/0/3
```

Vlan(id):1024.

```
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
```

Router port(s):total 1 port.

```
GE1/0/1 (D)
```

IP group(s):the following ip group(s) match to one mac group.

```
IP group address: FF1E::101
( :, FF1E::101):
```

Host port(s):total 0 port.

```
MAC group(s):
  MAC group address: 3333-0000-0101
```

```
Host port(s):total 0 port.
```

The output shows that:

- MLD snooping in the IPv6 multicast VLAN (VLAN 1024) maintains the router ports.
- MLD snooping in the sub-VLANs (VLAN 2 through VLAN 5) maintains the member ports.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
  ipv6
#
  mld-snooping
#
vlan 2 to 5
#
vlan 1024
  mld-snooping enable
#
multicast-vlan ipv6 1024
  subvlan 2 to 5
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port access vlan 1024
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 2 to 3
#
interface GigabitEthernet1/0/3
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 4 to 5
```

Example: Configuring a port-based IPv6 multicast VLAN

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

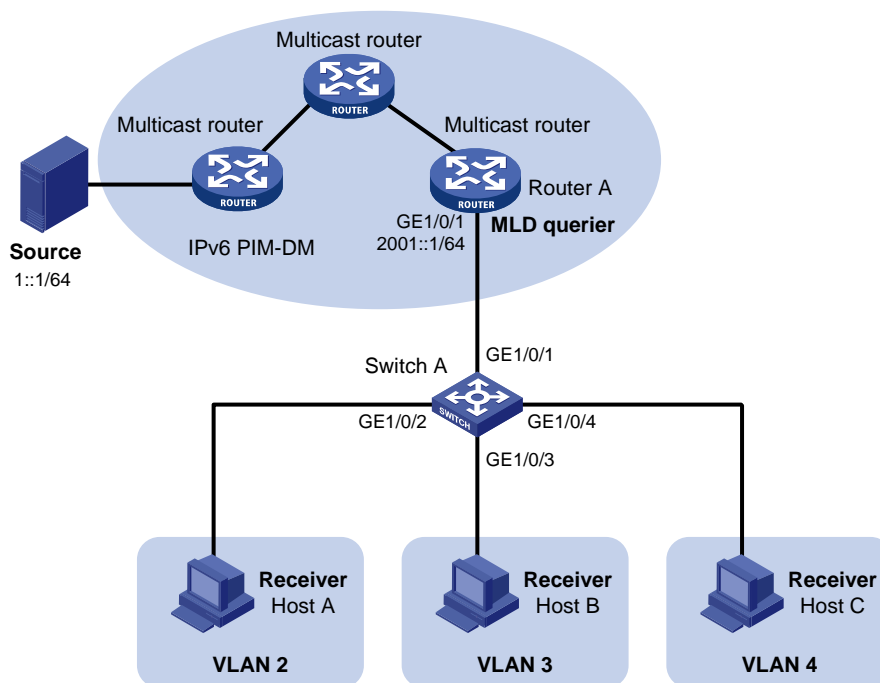
Network requirements

As shown in [Figure 88](#):

- The Layer 2 user network is connected to the MLD querier (Router A) in the IPv6 PIM-DM domain through Switch A.
- Each user VLAN has a receiver that belongs to the same IPv6 multicast group. The receiver hosts are directly connected to Switch A.

To save bandwidth and reduce the burden on Layer 3 multicast routers, configure a port-based multicast VLAN on Switch A. In this scenario, Layer 3 multicast routers only need to send multicast data to the multicast VLAN. The receiver hosts in different user VLANs can receive the data.

Figure 88 Network diagram



Configuration restrictions and guidelines

When you configure a port-based IPv6 multicast VLAN, follow these restrictions and guidelines:

- The VLAN to be configured as the IPv6 multicast VLAN must exist.
- A port can belong to only one IPv6 multicast VLAN.
- You must enable MLD snooping for the IPv6 multicast VLAN and the user VLANs.
- The user ports must be hybrid ports. You must assign user ports to the IPv6 multicast VLAN and user VLANs as untagged VLAN members.

Configuration procedures

1. Enable IPv6 forwarding on the switches. (Details not shown.)
2. Configure Switch A:

Enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

Create VLAN 1024, and assign GigabitEthernet 1/0/1 to the VLAN.

```
[SwitchA] vlan 1024
[SwitchA-vlan1024] port gigabitethernet 1/0/1
```

Enable MLD snooping for VLAN 1024.

```
[SwitchA-vlan1024] mld-snooping enable
[SwitchA-vlan1024] quit
```

Create VLAN 2, and enable MLD snooping for this VLAN.

```
[SwitchA] vlan 2
[SwitchA-vlan2] mld-snooping enable
[SwitchA-vlan2] quit
```

Configure VLAN 3 and VLAN 4 in the same way. (Details not shown.)

Configure GigabitEthernet 1/0/2 as a hybrid port, and configure VLAN 2 as the PVID.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type hybrid
[SwitchA-GigabitEthernet1/0/2] port hybrid pvid vlan 2
```

Assign GigabitEthernet 1/0/2 to VLAN 2 and VLAN 1024 as an untagged VLAN member.

```
[SwitchA-GigabitEthernet1/0/2] port hybrid vlan 2 1024 untagged
[SwitchA-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as a hybrid port, and configure VLAN 3 as the PVID.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type hybrid
[SwitchA-GigabitEthernet1/0/3] port hybrid pvid vlan 3
```

Assign GigabitEthernet 1/0/3 to VLAN 3 and VLAN 1024 as an untagged VLAN member.

```
[SwitchA-GigabitEthernet1/0/3] port hybrid vlan 3 1024 untagged
[SwitchA-GigabitEthernet1/0/3] quit
# Configure GigabitEthernet 1/0/4 as a hybrid port, and configure VLAN 4 as the PVID.
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-type hybrid
[SwitchA-GigabitEthernet1/0/4] port hybrid pvid vlan 4
# Assign GigabitEthernet 1/0/4 to VLAN 4 and VLAN 1024 as an untagged VLAN member.
[SwitchA-GigabitEthernet1/0/4] port hybrid vlan 4 1024 untagged
[SwitchA-GigabitEthernet1/0/4] quit
# Configure VLAN 1024 as the IPv6 multicast VLAN.
[SwitchA] multicast-vlan ipv6 1024
# Assign GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 to VLAN 1024.
[SwitchA-ipv6-mvlan-1024] port gigabitethernet 1/0/2 to gigabitethernet 1/0/4
[SwitchA-ipv6-mvlan-1024] quit
```

Verifying the configuration

1. Send MLD reports from the receiver hosts in the user VLANs to join the IPv6 multicast group **FF1E::101**. (Details not shown.)
2. Verify that Switch A can receive the reports and that it can forward the reports to Router A.

Display information about the IPv6 multicast VLAN.

```
[SwitchA] display multicast-vlan ipv6
Total 1 IPv6 multicast-vlan(s)
```

```
IPv6 multicast vlan 1024
```

```
subvlan list:
```

```
no subvlan
```

```
port list:
```

```
GE1/0/2
```

```
GE1/0/3
```

```
GE1/0/4
```

Display MLD snooping group information.

```
[SwitchA] display mld-snooping group
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
```

```
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
Vlan(id):1024.
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Router port(s):total 1 port.
```

```
GE1/0/1
```

```
(D)
```


IP group(s):the following ip group(s) match to one mac group.

IP group address: FF1E::101

(::, FF1E::101):

Host port(s):total 3 port.

GE1/0/2 (D)

GE1/0/3 (D)

GE1/0/4 (D)

MAC group(s):

MAC group address: 3333-0000-0101

Host port(s):total 3 port.

GE1/0/2

GE1/0/3

GE1/0/4

The output shows that MLD snooping is maintaining router ports and member ports in the IPv6 multicast VLAN (VLAN 1024).

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
  ipv6
#
mld-snooping
#
vlan 2
  mld-snooping enable
#
vlan 3
  mld-snooping enable
#
vlan 4
  mld-snooping enable
#
vlan 1024
  mld-snooping enable
#
multicast-vlan ipv6 1024
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port access vlan 1024
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port link-type hybrid
  port hybrid vlan 1 to 2 1024 untagged
  port hybrid pvid vlan 2
```

```
port multicast-vlan ipv6 1024
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type hybrid
port hybrid vlan 1 3 1024 untagged
port hybrid pvid vlan 3
port multicast-vlan ipv6 1024
#
interface GigabitEthernet1/0/4
port link-mode bridge
port link-type hybrid
port hybrid vlan 1 4 1024 untagged
port hybrid pvid vlan 4
port multicast-vlan ipv6 1024
```

IPv6 PIM configuration examples

This chapter provides IPv6 PIM configuration examples.

Based on the implementation mechanism, IPv6 PIM includes the following categories:

- **Protocol Independent Multicast–Dense Mode for IPv6**—IPv6 PIM-DM uses the ASM model and is suitable for small-sized IPv6 networks with densely distributed multicast members.
- **Protocol Independent Multicast–Sparse Mode for IPv6**—IPv6 PIM-SM uses the ASM model and is suitable for large- and medium-sized IPv6 networks with sparsely and widely distributed multicast members. For refined management, IPv6 PIM-SM employs the IPv6 administrative scoping mechanism to provide services for private IPv6 group addresses in specific admin-scoped zones.
- **Protocol Independent Multicast Source-Specific Multicast for IPv6**—IPv6 PIM-SSM provides a solution for IPv6 source-specific multicast.

General configuration restrictions and guidelines

When you configure IPv6 PIM, follow these restrictions and guidelines:

- All the interfaces on a switch must operate in the same IPv6 PIM mode.
- If a VLAN is running a Layer 2 multicast protocol, do not configure Layer 3 multicast protocols on the VLAN interface of this VLAN.

Example: Configuring IPv6 PIM-DM

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

Network requirements

As shown in [Figure 89](#):

- All the switches are Layer 3 switches, and they run OSPFv3.
- The IPv6 multicast source, receiver hosts, and switches can communicate with each other through IPv6 unicast routes.

Configure IPv6 PIM-DM on each switch, so that multicast data can be sent to receiver hosts in **N1** and **N2**.

Figure 89 Network diagram

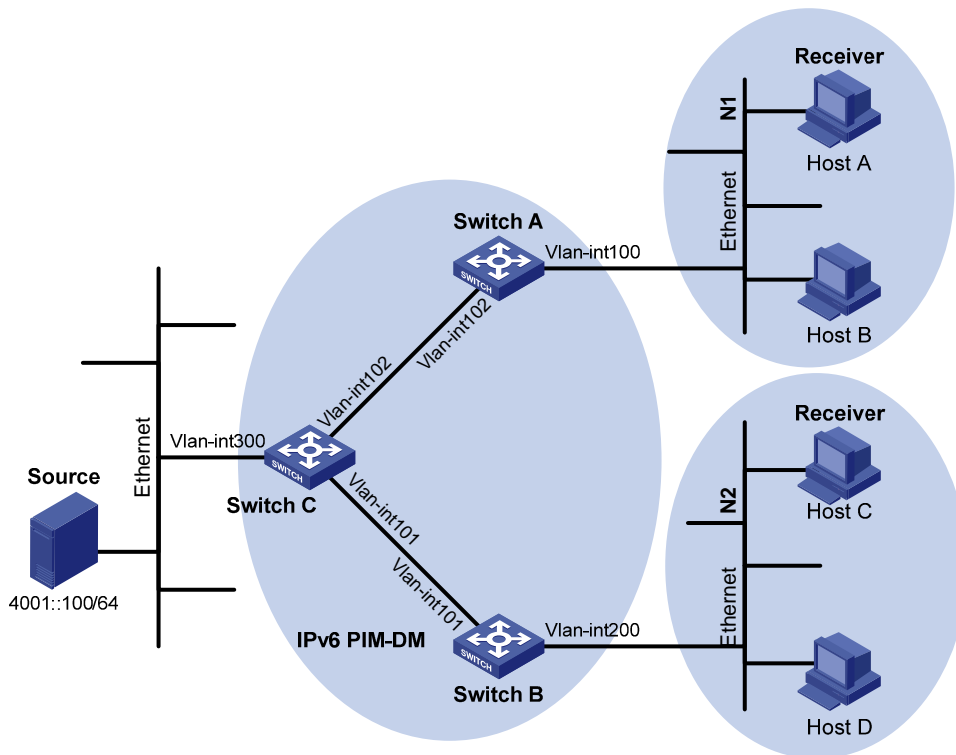


Table 3 Interface and IPv6 address assignment

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. Enable IPv6 forwarding on the switches. (Details not shown.)

2. Assign an IPv6 address and prefix length to each interface according to [Table 3](#). (Details not shown.)
3. Configure OSPFv3 on the switches in the IPv6 PIM-DM domain. (Details not shown.)
4. Enable IPv6 multicast routing and IPv6 PIM-DM:

On Switch A, enable IPv6 multicast routing globally.

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
```

On Switch A, enable IPv6 PIM-DM on each interface.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim ipv6 dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim ipv6 dm
[SwitchA-Vlan-interface102] quit
```

On Switch B and Switch C, enable IPv6 multicast routing and IPv6 PIM-DM in the same way Switch A is configured. (Details not shown.)

5. Enable MLD on the interfaces connected to the stub networks **N1** and **N2**:

On Switch A, enable MLD (MLDv1 by default) on VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] quit
```

On Switch B, enable MLD on VLAN-interface 200 in the same way Switch A is configured. (Details not shown.)

Verifying the configuration

1. Send MLDv1 reports from Host A and Host C to join the IPv6 multicast group **FF0E::101**. (Details not shown.)
2. Send IPv6 multicast data from the IPv6 multicast source **4001::100/64** to the IPv6 multicast group. (Details not shown.)
3. Verify that correct IPv6 PIM routing information can be created on each switch. This configuration takes Switch A and Switch C as examples:

Display information about the IPv6 PIM routing table on Switch C.

```
[SwitchC] display pim ipv6 routing-table
Total 0 (*, G) entry; 1 (S, G) entry
```

```
(4001::100, FF0E::101)
```

```
Protocol: pim-dm, Flag: LOC ACT
UpTime: 00:02:19
Upstream interface: Vlan-interface300
Upstream neighbor: NULL
RPF prime neighbor: NULL
```

```

Downstream interface(s) information:
Total number of downstreams: 2
  1: Vlan-interface101
      Protocol: pim-dm, UpTime: 00:02:19, Expires: never
  2: Vlan-interface102
      Protocol: pim-dm, UpTime: 00:02:19, Expires: never

# Display information about the IPv6 PIM routing table on Switch A.
[SwitchA] display pim ipv6 routing-table
Total 1 (*, G) entry; 1 (S, G) entry

(*, FF0E::101)
  Protocol: pim-dm, Flag: WC
  UpTime: 00:01:24
  Upstream interface: NULL
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface100
        Protocol: mld, UpTime: 00:01:20, Expires: never

(4001::100, FF0E::101)
  Protocol: pim-dm, Flag: ACT
  UpTime: 00:01:20
  Upstream interface: Vlan-interface102
    Upstream neighbor: FE80::20F:E2FF:FE67:B323
    RPF prime neighbor: FE80::20F:E2FF:FE67:B323
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface100
        Protocol: pim-dm, UpTime: 00:01:20, Expires: never

```

The output shows that:

- An SPT is established through traffic flooding. Switches on the SPT paths (Switch A and Switch B) have their (S, G) entries.
- Because Host A sends an MLD report to Switch A to join the IPv6 multicast group, a (*, G) entry is generated on Switch A.

Configuration files

- Switch A:


```

#
ipv6
#
multicast ipv6 routing-enable
#
vlan 100

```

```

#
vlan 102
#
interface Vlan-interface100
  ipv6 address 1001::1/64
  ospfv3 1 area 0.0.0.0
  mld enable
  pim ipv6 dm
#
interface Vlan-interface102
  ipv6 address 1002::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 dm
#
ospfv3 1
  router-id 1.1.1.1
  area 0.0.0.0
#

```

- Switch B:

```

#
  ipv6
#
  multicast ipv6 routing-enable
#
vlan 101
#
vlan 200
#
interface Vlan-interface101
  ipv6 address 2002::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 dm
#
interface Vlan-interface200
  ipv6 address 2001::1/64
  ospfv3 1 area 0.0.0.0
  mld enable
  pim ipv6 dm
#
ospfv3 1
  router-id 2.2.2.2
  area 0.0.0.0
#

```

- Switch C:

```

#
  ipv6
#
  multicast ipv6 routing-enable

```

```

#
vlan 101 to 102
#
vlan 300
#
interface Vlan-interface101
  ipv6 address 2002::2/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 dm
#
interface Vlan-interface102
  ipv6 address 1002::2/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 dm
#
interface Vlan-interface300
  ipv6 address 4001::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 dm
#
ospfv3 1
  router-id 3.3.3.3
  area 0.0.0.0
#

```

Example: Configuring IPv6 PIM-SM

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

Network requirements

As shown in [Figure 90](#):

- All the switches are Layer 3 switches, and they run OSPFv3.
- The multicast source, receiver hosts, and switches can communicate with each other through IPv6 unicast routes.

Configure IPv6 PIM-SM on each switch so that multicast data of the multicast groups in the range of **FF0E::/64** can be sent to receivers in **N1** and **N2**.

Figure 90 Network diagram

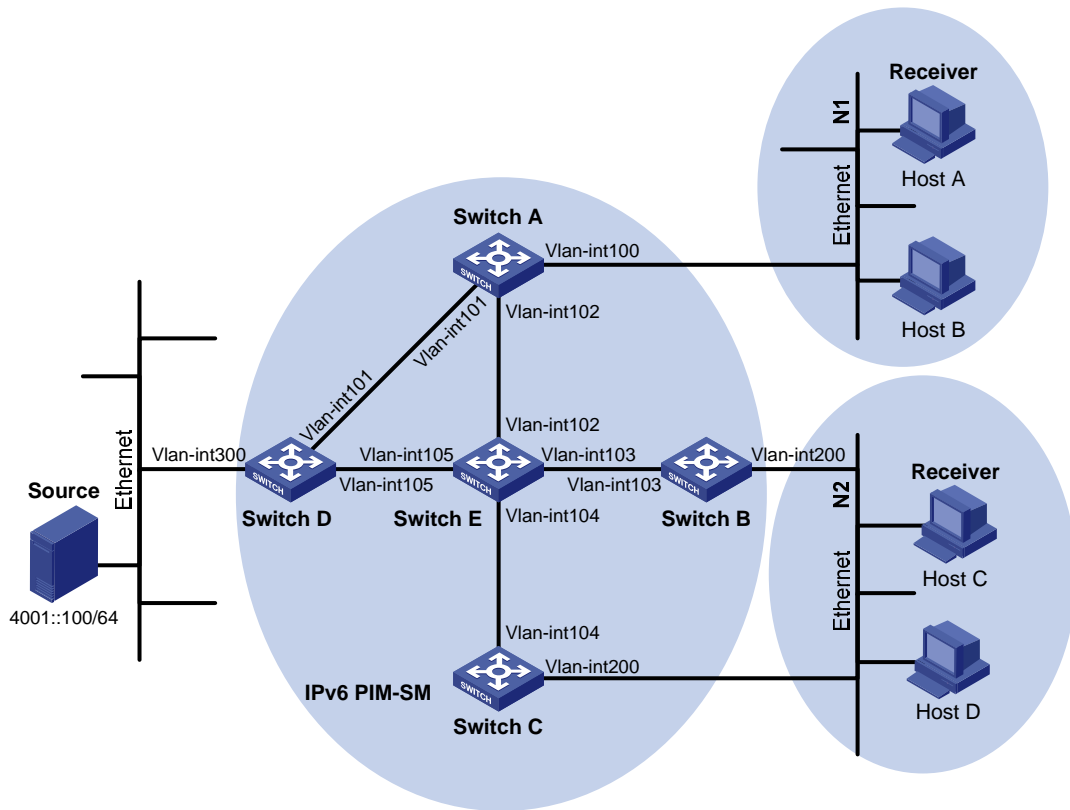


Table 4 Interface and IPv6 address assignment

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
Switch D	VLAN-interface 105	4002::1/64
Switch E	VLAN-interface 104	3001::2/64
Switch E	VLAN-interface 103	2002::2/64
Switch E	VLAN-interface 102	1003::2/64
Switch E	VLAN-interface 105	4002::2/64

Requirements analysis

Because receivers request multicast data of the multicast groups in the range of **FF0E::/64**, you must configure C-RPs to provide services for this group range.

To lessen the burden on a single RP, configure multiple C-RPs on the IPv6 network. For example, configure Switch D and Switch E as C-RPs so they can provide services for different multicast groups through the bootstrap mechanism.

To avoid communication interruption caused by single-point failure of the BSR, configure multiple C-BSRs on the IPv6 network. For example, you can configure a C-BSR on a switch that acts as a C-RP. When the BSR fails, other C-BSRs can elect a new BSR.

Configuration restrictions and guidelines

When you configure IPv6 PIM-SM, follow these restrictions and guidelines:

- On a shared-media network with multiple Layer 3 switches connected, configure MLD and IPv6 PIM-SM on each Layer 3 switch to avoid communication interruption. In this way, 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. Enable IPv6 forwarding on the switches. (Details not shown.)
2. Assign an IPv6 address and prefix length to each interface according to [Table 4](#). (Details not shown.)
3. Configure OSPFv3 on the switches in the IPv6 PIM-SM domain. (Details not shown.)
4. Enable IPv6 multicast routing globally and configure IPv6 PIM-SM:

On Switch A, enable IPv6 multicast routing globally.

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
```

On Switch A, enable IPv6 PIM-SM on each interface.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
```

```
[SwitchA-Vlan-interface102] pim ipv6 sm
[SwitchA-Vlan-interface102] quit
```

On Switch B, Switch C, Switch D, and Switch E, enable IPv6 multicast routing and IPv6 PIM-SM in the same way Switch A is configured. (Details not shown.)

5. Enable MLD on the interfaces connected to the stub networks **N1** and **N2**:

On Switch A, enable MLD (MLDv1 by default) on VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] quit
```

On Switch B and Switch C, enable MLD on VLAN-interface 200 in the same way Switch A is configured. (Details not shown.)

6. Configure C-BSRs and C-RPs:

On Switch D, create an IPv6 ACL to define an IPv6 multicast group range to which the C-RP is designated.

```
<SwitchD> system-view
[SwitchD] acl ipv6 number 2005
[SwitchD-aclv6-basic-2005] rule permit source ff0e:: 64
[SwitchD-aclv6-basic-2005] quit
```

On Switch D, configure VLAN-interface 105 as a C-RP. Reference ACL 2005 to provide services for only the multicast groups in the range of **FF0E::/64**.

```
[SwitchD] pim ipv6
[SwitchD-pim6] c-rp 4002::1 group-policy 2005
```

On Switch D, configure VLAN-interface 105 as a C-BSR. Set its hash mask length and priority to **128** and **10**, respectively.

```
[SwitchD-pim6] c-bsr 4002::1 128 10
[SwitchD-pim6] quit
```

On Switch E, create an IPv6 ACL to define an IPv6 multicast group range to which the C-RP is designated.

```
<SwitchE> system-view
[SwitchE] acl ipv6 number 2005
[SwitchE-acl6-basic-2005] rule permit source ff0e:: 64
[SwitchE-acl6-basic-2005] quit
```

On Switch E, configure VLAN-interface 102 as a C-RP. Reference ACL 2005 to provide services for only the multicast groups in the range of **FF0E::/64**.

```
[SwitchE] pim ipv6
[SwitchE-pim6] c-rp 1003::2 group-policy 2005
```

On Switch E, configure VLAN-interface 102 as a C-BSR. Set its hash mask length and priority to **128** and **20**, respectively.

```
[SwitchE-pim6] c-bsr 1003::2 128 20
[SwitchE-pim6] quit
```

Verifying the configuration

1. Verify that the MLD querier and the DR are correctly elected on the shared-media network **N2**:

Display MLD querier information on Switch B.

```
[SwitchB] display mld interface
Interface information of VPN-Instance: public net
Vlan-interface200(FE80::223:89FF:FE5F:958B):
  MLD is enabled
  Current MLD version is 1
  Value of query interval for MLD(in seconds): 125
  Value of other querier present interval for MLD(in seconds): 255
  Value of maximum query response time for MLD(in seconds): 10
  Querier for MLD: FE80::223:89FF:FE5F:958B (this router)
  Total 1 MLD Group reported
```

Display MLD querier information on Switch C.

```
[SwitchC] display mld interface
Interface information of VPN-Instance: public net
Vlan-interface200(FE80::223:89FF:FE5F:958C):
  MLD is enabled
  Current MLD version is 1
  Value of query interval for MLD(in seconds): 125
  Value of other querier present interval for MLD(in seconds): 255
  Value of maximum query response time for MLD(in seconds): 10
  Querier for MLD: FE80::223:89FF:FE5F:958B
  Total 1 MLD Group reported
```

The output shows that Switch B is elected 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 pim ipv6 interface
VPN-Instance: public net


| Interface | NbrCnt | HelloInt | DR-Pri | DR-Address                   |
|-----------|--------|----------|--------|------------------------------|
| Vlan103   | 1      | 30       | 1      | FE80::223:89FF:<br>FE5F:958E |
| Vlan200   | 1      | 30       | 1      | FE80::223:89FF:<br>FE5F:958C |


```

Display IPv6 PIM information on Switch C.

```
[SwitchC] display pim ipv6 interface
VPN-Instance: public net


| Interface | NbrCnt | HelloInt | DR-Pri | DR-Address                           |
|-----------|--------|----------|--------|--------------------------------------|
| Vlan104   | 1      | 30       | 1      | FE80::223:89FF:<br>FE5F:958E         |
| Vlan200   | 1      | 30       | 1      | FE80::223:89FF:<br>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. (Details not shown.)
 - c. Display IPv6 PIM routing table information on the switches. This configuration takes Switch A, Switch C, and Switch D as examples:

Display information about the IPv6 PIM routing table on Switch A.

```
[SwitchA] display pim ipv6 routing-table
VPN-Instance: public net
Total 1 (*, G) entry; 1 (S, G) entry
```

```
(*, FF0E::100)
```

```
RP: 1003::2
```

```
Protocol: pim-sm, Flag: WC
```

```
UpTime: 00:03:45
```

```
Upstream interface: Vlan-interface102
```

```
Upstream neighbor: FE80::223:89FF:FE5F:958E
```

```
RPF prime neighbor: FE80::223:89FF:FE5F:958E
```

```
Downstream interface(s) information:
```

```
Total number of downstreams: 1
```

```
1: Vlan-interface100
```

```
Protocol: mld, UpTime: 00:02:15, Expires: 00:03:06
```

```
(4001::100, FF0E::100)
```

```
RP: 1003::2
```

```
Protocol: pim-sm, Flag: SPT ACT
```

```
UpTime: 00:02:15
```

```
Upstream interface: Vlan-interface101
```

```
Upstream neighbor: FE80::223:89FF:FE5F:958D
```

```
RPF prime neighbor: FE80::223:89FF:FE5F:958D
```

```
Downstream interface(s) information:
```

```
Total number of downstreams: 1
```

```
1: Vlan-interface100
```

```
Protocol: pim-sm, UpTime: 00:02:15, Expires: 00:03:06
```

Display information about the IPv6 PIM routing table on Switch D.

```
[SwitchD] display pim ipv6 routing-table
VPN-Instance: public net
Total 0 (*, G) entry; 1 (S, G) entry
```

```
(4001::100, FF0E::100)
```

```
RP: 1003::2
```

```

Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 00:14:44
Upstream interface: Vlan-interface300
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 1
    1: Vlan-interface101
        Protocol: mld, UpTime: 00:14:44, Expires: 00:02:26

```

Display information about the IPv6 PIM routing table on Switch E.

```

[SwitchE] display pim ipv6 routing-table
VPN-Instance: public net
Total 1 (*, G) entry; 1 (S, G) entry

```

```
(*, FF0E::100)
```

```
RP: 1003::2 (local)
```

```

Protocol: pim-sm, Flag: WC
UpTime: 00:16:56
Upstream interface: Register
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 1
    1: Vlan-interface102
        Protocol: pim-sm, UpTime: 00:16:56, Expires: 00:02:34

```

```
(4001::100, FF0E::100)
```

```
RP: 1003::2 (local)
```

```

Protocol: pim-sm, Flag: RPT SPT ACT
UpTime: 00:25:32
Upstream interface: Vlan-interface105
    Upstream neighbor: FE80::223:89FF:FE5F:958D
    RPF prime neighbor: FE80::223:89FF:FE5F:958D
Downstream interface(s) information: None

```

The output shows that:

- The RP for the multicast group **FF0E::100** is Switch E as a result of hash calculation.
- An SPT has been built between the source-side DR (Switch D) and the RP (Switch E).
- An RPT has been built between the receiver-side DR (Switch A) and the RP (Switch E), and Switch A and Switch E have created (*, G) entries. After receiving IPv6 multicast data, the receiver-side DR (Switch A) immediately switches from the RPT to the SPT.

A new SPT is built between the receiver-side DR (Switch A) and the source-side DR (Switch D). The switches (Switch A and Switch D) on the new SPT path have their (S, G) entries.

Configuration files

- Switch A:

```
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 100 to 102
#
interface Vlan-interface100
  ipv6 address 1001::1/64
  ospfv3 1 area 0.0.0.0
  mld enable
  pim ipv6 sm
#
interface Vlan-interface101
  ipv6 address 1002::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
interface Vlan-interface102
  ipv6 address 1003::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
ospfv3 1
  router-id 1.1.1.1
  area 0.0.0.0
#
```

- Switch B:

```
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 103
#
vlan 200
#
interface Vlan-interface103
  ipv6 address 2002::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
interface Vlan-interface200
  ipv6 address 2001::1/64
```

```
ospfv3 1 area 0.0.0.0
mld enable
pim ipv6 sm
#
ospfv3 1
router-id 2.2.2.2
area 0.0.0.0
#
```

- Switch C:

```
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 104
#
vlan 200
#
interface Vlan-interface104
ipv6 address 3001::1/64
ospfv3 1 area 0.0.0.0
pim ipv6 sm
#
interface Vlan-interface200
ipv6 address 2001::2/64
ospfv3 1 area 0.0.0.0
mld enable
pim ipv6 sm
#
ospfv3 1
router-id 3.3.3.3
area 0.0.0.0
#
```

- Switch D:

```
#
ipv6
#
multicast ipv6 routing-enable
#
acl ipv6 number 2005
rule 0 permit source FF0E::/64
#
vlan 101
#
vlan 105
#
vlan 300
#
```



```

interface Vlan-interface101
  ipv6 address 1002::2/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
interface Vlan-interface105
  ipv6 address 4002::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
interface Vlan-interface300
  ipv6 address 4001::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
pim ipv6
  c-bsr hash-length 128
  c-bsr priority 10
  c-bsr 4002::1
  c-rp 4002::1 group-policy 2005
#
ospfv3 1
  router-id 4.4.4.4
  area 0.0.0.0
#

```

- Switch E:

```

#
ipv6
#
multicast ipv6 routing-enable
#
acl ipv6 number 2005
  rule 0 permit source FF0E::/64
#
vlan 102 to 104
#
vlan 105
#
interface Vlan-interface102
  ipv6 address 1003::2/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
interface Vlan-interface103
  ipv6 address 2002::2/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#

```

```

interface Vlan-interface104
  ipv6 address 3001::2/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
interface Vlan-interface105
  ipv6 address 4002::2/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
pim ipv6
c-bsr hash-length 128
c-bsr priority 20
c-bsr 1003::2
c-rp 1003::2 group-policy 2005
#
ospfv3 1
  router-id 5.5.5.5
  area 0.0.0.0
#

```

Example: Configuring IPv6 PIM-SM admin-scoped zones

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

Network requirements

As shown in [Figure 91](#):

- All switches are Layer 3 switches, and they run OSPFv3.
- Multicast sources, receiver hosts, and switches can communicate with each other through unicast routes.

Use the IPv6 PIM-SM administrative scoping mechanism to 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 IPv6 multicast groups with the scope field of 4. Source 1 in admin-scoped zone 1 and Source 2 in admin-scoped zone 2 send multicast data only

to these IPv6 multicast groups. Receivers in each admin-scoped zone can request multicast data only within the local zone.

- Source 3 in the global-scoped zone sends multicast data to all multicast groups with the scope field value of **14**. All receivers on the network can request multicast data of these multicast groups.

Figure 91 Network diagram

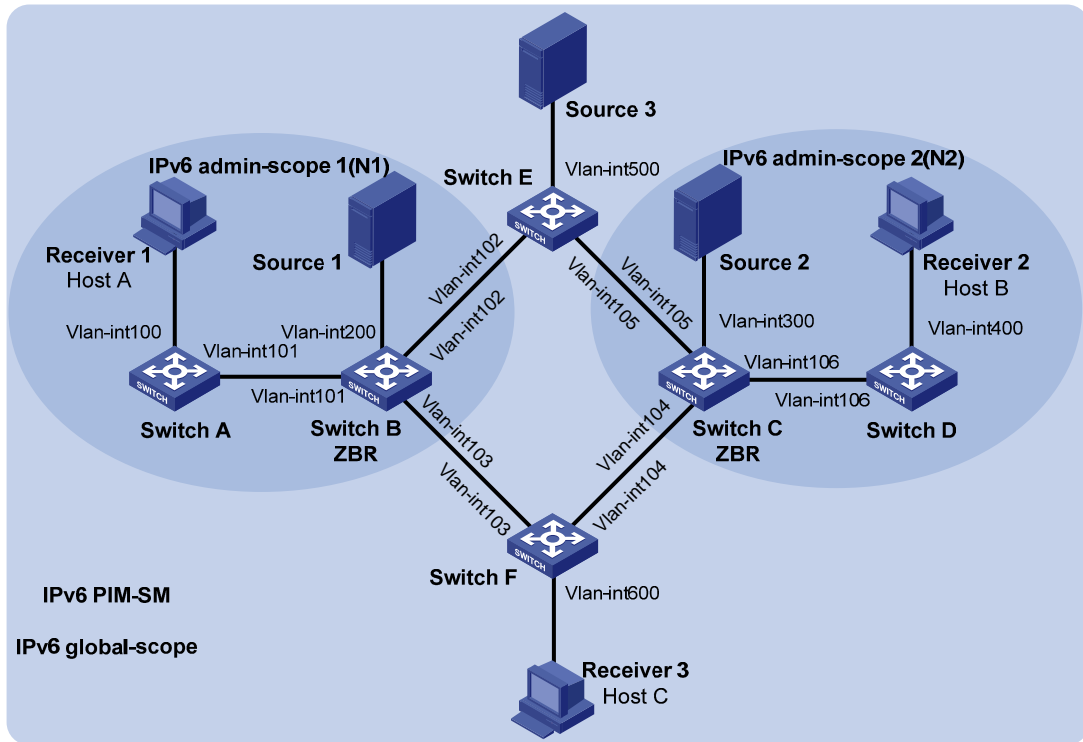


Table 5 Interface and IPv6 address assignment

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
Switch B	VLAN-interface 102	1003::1/64	Switch F	VLAN-interface 600	6001::1/64
Switch B	VLAN-interface 103	1004::1/64	Switch F	VLAN-interface 103	1004::2/64
Switch C	VLAN-interface 300	3001::1/64	Switch F	VLAN-interface 104	1005::2/64
Switch C	VLAN-interface 104	1005::1/64	Source 1	N/A	2001::100/64
Switch C	VLAN-interface 105	1006::1/64	Source 2	N/A	3001::100/64
Switch C	VLAN-interface 106	1007::1/64	Source 3	N/A	5001::100/64
Switch D	VLAN-interface 400	4001::1/64			

Requirements analysis

To divide different admin-scoped zones, 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 IPv6 multicast groups, configure C-BSRs and C-RPs in each zone as follows:

- The C-BSRs and C-RPs in each admin-scoped zone provide services for the IPv6 multicast groups to which the admin-scoped zone is designated.
- The C-BSRs and C-RPs in the global-scoped zone provide services for all IPv6 multicast groups except multicast groups to which admin-scoped zones are designated.

Configuration restrictions and guidelines

When you configure IPv6 PIM-SM admin-scoped zones, follow these restrictions and guidelines:

- To establish and maintain IPv6 multicast group membership at Layer 3, enable MLD on the interfaces of switches that are directly connected to receiver hosts.
- Before you configure IPv6 admin-scoped zones, enable IPv6 administrative scoping on all Layer 3 switches in the IPv6 PIM-SM domain.

Configuration procedures

1. Enable IPv6 forwarding on the switches. (Details not shown.)
2. Assign an IPv6 address and prefix length to each interface according to [Table 5](#). (Details not shown.)
3. Configure OSPFv3 on the switches in the IPv6 PIM-SM domain. (Details not shown.)
4. Enable IPv6 multicast routing, IPv6 administrative scoping, and IPv6 PIM-SM:

On Switch A, enable IPv6 multicast routing globally.

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
```

On Switch A, enable IPv6 administrative scoping globally.

```
[SwitchA] pim ipv6
[SwitchA-pim6] c-bsr admin-scope
[SwitchA-pim6] quit
```

On Switch A, enable IPv6 PIM-SM on each interface.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
[SwitchA-Vlan-interface101] quit
```

On Switch B, Switch C, Switch D, Switch E, and Switch F, enable IPv6 multicast routing, IPv6 administrative scoping, and IPv6 PIM-SM in the same way Switch A is configured. (Details not shown.)

5. Enable MLD on the interfaces connected to the receiver hosts:

On Switch A, enable MLD on VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface101] quit
```

On Switch D and Switch F, enable MLD in the same way Switch A is configured. (Details not shown.)

6. Configure IPv6 admin-scoped zone boundaries:

On Switch B, configure VLAN-interface 102 and VLAN-interface 103 as the boundaries of IPv6 admin-scoped zone 1.

```
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] multicast ipv6 boundary scope 4
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] multicast ipv6 boundary scope 4
[SwitchB-Vlan-interface103] quit
```

On Switch C, configure VLAN-interface 104 and VLAN-interface 105 as the boundaries of IPv6 admin-scoped zone 2.

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 104
[SwitchC-Vlan-interface104] multicast ipv6 boundary scope 4
[SwitchC-Vlan-interface104] quit
[SwitchC] interface vlan-interface 105
[SwitchC-Vlan-interface105] multicast ipv6 boundary scope 4
[SwitchC-Vlan-interface105] quit
```

7. Configure C-BSRs and C-RPs:

On Switch B, configure the C-BSR service scope as IPv6 admin-scoped zone 1. Configure VLAN-interface 101 as a C-BSR for this zone.

```
[SwitchB] pim ipv6
[SwitchB-pim6] c-bsr scope 4
[SwitchB-pim6] c-bsr 1002::2
```

On Switch B, configure VLAN-interface 101 as a C-RP for IPv6 admin-scoped zone 1.

```
[SwitchB-pim6] c-rp 1002::2 scope 4
[SwitchB-pim6] quit
```

On Switch C, configure the C-BSR service scope as IPv6 admin-scoped zone 2. Configure VLAN-interface 104 as a C-BSR for this zone.

```
[SwitchC] pim ipv6
[SwitchC-pim6] c-bsr scope 4
[SwitchC-pim6] c-bsr 1007::1
```

On Switch C, configure VLAN-interface 104 as a C-RP for IPv6 admin-scoped zone 2.

```
[SwitchC-pim6] c-rp 1007::1 scope 4
[SwitchC-pim6] quit
```

On Switch E, configure VLAN-interface 102 as a C-BSR and a C-RP for the IPv6 global-scoped zone.

```
<SwitchE> system-view
[SwitchE] pim ipv6
[SwitchE-pim6] c-bsr scope global
[SwitchE-pim6] c-bsr 1003::2
[SwitchE-pim6] c-rp 1003::2
[SwitchE-pim6] quit
```

Verifying the configuration

1. Verify that the BSR has been elected and that the local C-RP configuration in each zone has taken effect:

On Switch B, display information about the BSR and the locally configured C-RP.

```
[SwitchB] display pim ipv6 bsr-info
VPN-Instance: public net
Elected BSR Address: 1002::2
  Priority: 64
  Hash mask length: 126
  State: Elected
  Scope: 4
  Uptime: 00:03:13
  Next BSR message scheduled at: 00:00:09
Elected BSR Address: 1003::2
  Priority: 10
  Hash mask length: 128
  State: Accept Preferred
  Scope: 14
  Uptime: 00:00:51
  Expires: 00:02:00
Candidate BSR Address: 1002::2
  Priority: 64
  Hash mask length: 126
  State: Elected
  Scope: 4

Candidate RP: 1002::2(Vlan-interface101)
  Priority: 192
  HoldTime: 150
  Advertisement Interval: 60
  Next advertisement scheduled at: 00:00:59
```

On Switch C, display information about the BSR and the locally configured C-RP.

```
[SwitchC] display pim ipv6 bsr-info
VPN-Instance: public net
```

```
Elected BSR Address: 1007::1
  Priority: 64
  Hash mask length: 126
  State: Elected
Scope: 4
  Uptime: 00:03:13
  Next BSR message scheduled at: 00:00:09
```

```
Elected BSR Address: 1003::2
  Priority: 10
  Hash mask length: 128
  State: Accept Preferred
Scope: 14
  Uptime: 00:00:51
  Expires: 00:02:00
```

```
Candidate BSR Address: 1007::1
  Priority: 64
  Hash mask length: 126
  State: Elected
Scope: 4
```

```
Candidate RP: 1007::1(Vlan-interface106)
  Priority: 192
  HoldTime: 150
  Advertisement Interval: 60
  Next advertisement scheduled at: 00:00:59
```

On Switch E, display information about the BSR and the locally configured C-RP.

```
[SwitchE] display pim ipv6 bsr-info
VPN-Instance: public net
```

```
Elected BSR Address: 1003::2
  Priority: 10
  Hash mask length: 128
  State: Elected
Scope: 14
  Uptime: 00:00:51
  Next BSR message scheduled at: 00:00:42
```

```
Candidate BSR Address: 1003::2
  Priority: 10
  Hash mask length: 128
  State: Elected
Scope: 14
```

```
Candidate RP: 1003::2(Vlan-interface102)
  Priority: 192
  HoldTime: 150
  Advertisement Interval: 60
  Next advertisement scheduled at: 00:00:59
```

2. Verify that the RP has been elected in each zone to provide services for different IPv6 multicast groups:

Display RP information on Switch B.

```
[SwitchB] display pim ipv6 rp-info
```

```
VPN-Instance: public net
```

```
PIM-SM BSR RP information:
```

```
prefix/prefix length: FF04::/16
```

```
RP: 1002::2 (local)
```

```
Priority: 192
```

```
HoldTime: 150
```

```
Uptime: 00:07:46
```

```
Expires: 00:01:44
```

```
prefix/prefix length: FF0E::/16
```

```
RP: 1003::2
```

```
Priority: 192
```

```
HoldTime: 150
```

```
Uptime: 00:03:36
```

```
Expires: 00:02:04
```

```
prefix/prefix length: FF14::/16
```

```
RP: 1002::2 (local)
```

```
Priority: 192
```

```
HoldTime: 150
```

```
Uptime: 00:07:47
```

```
Expires: 00:01:43
```

```
prefix/prefix length: FF1E::/16
```

```
RP: 1003::2
```

```
Priority: 192
```

```
HoldTime: 150
```

```
Uptime: 00:09:13
```

```
Expires: 00:02:27
```

The output for **FF24::/16** to **FFF4::/16** and **FF2E::/16** to **FFFE::/16** is omitted here.

Display RP information on Switch C.

```
[SwitchC] display pim ipv6 rp-info
```

```
VPN-Instance: public net
```

```
PIM-SM BSR RP information:
```

```
prefix/prefix length: FF04::/16
```

```
RP: 1007::1 (local)
```

```
Priority: 192
```

```
HoldTime: 150
```

```
Uptime: 00:07:46
```

```
Expires: 00:01:44
```

```
prefix/prefix length: FF0E::/16
```

```
RP: 1003::2
```

```
Priority: 192
```

```
HoldTime: 150
```


Uptime: 00:03:36
Expires: 00:02:04

prefix/prefix length: FF14::/16

RP: 1007::1 (local)
Priority: 192
HoldTime: 150
Uptime: 00:07:47
Expires: 00:01:43

prefix/prefix length: FF1E::/16

RP: 1003::2
Priority: 192
HoldTime: 150
Uptime: 00:09:13
Expires: 00:02:27

The output for **FF24::/16** to **FFF4::/16** and **FF2E::/16** to **FFFE::/16** is omitted here.

Display RP information on Switch E.

[SwitchE] display pim ipv6 rp-info

VPN-Instance: public net
PIM-SM BSR RP information:

prefix/prefix length: FF0E::/16

RP: 1003::2 (local)
Priority: 192
HoldTime: 150
Uptime: 00:03:36
Expires: 00:02:04

prefix/prefix length: FF1E::/16

RP: 1003::2 (local)
Priority: 192
HoldTime: 150
Uptime: 00:09:13
Expires: 00:02:27

The output for **FF2E::/16** to **FFFE::/16** is omitted here.

Display RP information on Switch F.

[SwitchF] display pim ipv6 rp-info

VPN-Instance: public net
PIM-SM BSR RP information:

prefix/prefix length: FF0E::/16

RP: 1003::2
Priority: 192
HoldTime: 150
Uptime: 00:03:35
Expires: 00:02:02

prefix/prefix length: FF1E::/16

```
RP: 1003::2
Priority: 192
HoldTime: 150
Uptime: 00:09:13
Expires: 00:02:22
```

The output for **FF2E::/16** to **FFFE::/16** is omitted here.

The output shows that:

- When a host in IPv6 admin-scoped zone 1 joins an IPv6 multicast group in the range of **FF04::/16** to **FFF4::/16**, the RP (Switch B) provides services for this multicast group locally.
- When a host in IPv6 admin-scoped zone 2 joins an IPv6 multicast group in the range of **FF04::/16** to **FFF4::/16**, the RP (Switch C) provides services for this multicast group locally.
- When a host in an IPv6 admin-scoped zone or the global-scoped zone joins an IPv6 multicast group in the range of **FF0E::/16** to **FFFE::/16**, the RP (Switch E) provides services for this multicast group.

Configuration files

- Switch A:

```
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
  ipv6 address 1001::1/64
  ospfv3 1 area 0.0.0.0
  mld enable
  pim ipv6 sm
#
interface Vlan-interface101
  ipv6 address 1002::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
ospfv3 1
  router-id 1.1.1.1
  area 0.0.0.0
#
pim ipv6
  c-bsr admin-scope
#
```

- Switch B:

```
#
```

```

ipv6
#
multicast ipv6 routing-enable
#
vlan 101 to 103
#
vlan 200
#
interface Vlan-interface101
  ipv6 address 1002::2/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
interface Vlan-interface102
  ipv6 address 1003::1/64
  ospfv3 1 area 0.0.0.0
  multicast ipv6 boundary scope 4
  pim ipv6 sm
#
interface Vlan-interface103
  ipv6 address 1004::1/64
  ospfv3 1 area 0.0.0.0
  multicast ipv6 boundary scope 4
  pim ipv6 sm
#
interface Vlan-interface200
  ipv6 address 2001::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
ospfv3 1
  router-id 2.2.2.2
  area 0.0.0.0
#
pim ipv6
  c-bsr admin-scope
  c-bsr scope 4
  c-bsr 1002::2
  c-rp 1002::2 scope 4
#

```

- Switch C:

```

#
ipv6
#
multicast ipv6 routing-enable
#
vlan 104 to 106
#

```

```

vlan 300
#
interface Vlan-interface104
  ipv6 address 1005::1/64
  ospfv3 1 area 0.0.0.0
  multicast ipv6 boundary scope 4
  pim ipv6 sm
#
interface Vlan-interface105
  ipv6 address 1006::1/64
  ospfv3 1 area 0.0.0.0
  multicast ipv6 boundary scope 4
  pim ipv6 sm
#
interface Vlan-interface106
  ipv6 address 1007::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
interface Vlan-interface300
  ipv6 address 3001::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
ospfv3 1
  router-id 3.3.3.3
  area 0.0.0.0
#
pim ipv6
  c-bsr admin-scope
  c-bsr scope 4
  c-bsr 1007::1
  c-rp 1007::1 scope 4
#

```

- Switch D:

```

#
ipv6
#
multicast ipv6 routing-enable
#
vlan 106
#
vlan 400
#
interface Vlan-interface106
  ipv6 address 1007::2/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm

```

```

#
interface Vlan-interface400
  ipv6 address 4001::1/64
  ospfv3 1 area 0.0.0.0
  mld enable
  pim ipv6 sm
#
ospfv3 1
  router-id 4.4.4.4
  area 0.0.0.0
#
pim ipv6
  c-bsr admin-scope
#

```

- Switch E:

```

#
ipv6
#
multicast ipv6 routing-enable
#
vlan 102
#
vlan 105
#
vlan 500
#
interface Vlan-interface102
  ipv6 address 1003::2/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
interface Vlan-interface105
  ipv6 address 1006::2/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
interface Vlan-interface500
  ipv6 address 5001::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
ospfv3 1
  router-id 5.5.5.5
  area 0.0.0.0
#
pim ipv6
  c-bsr admin-scope
  c-bsr scope 14

```

```

c-bsr hash-length 128
c-bsr priority 10
c-bsr 1003::2
c-rp 1003::2
#
• Switch F:
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 103 to 104
#
vlan 600
#
interface Vlan-interface103
  ipv6 address 1004::2/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
interface Vlan-interface104
  ipv6 address 1005::2/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
interface Vlan-interface600
  ipv6 address 6001::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
ospfv3 1
  router-id 6.6.6.6
  area 0.0.0.0
#
pim ipv6
  c-bsr admin-scope
#

```

Example: Configuring IPv6 PIM-SSM

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

Network requirements

As shown in [Figure 92](#):

- All switches are Layer 3 switches, and they run OSPFv3.
- Multicast sources, receiver hosts, and switches can communicate with each other through IPv6 unicast routes.
- The receiver hosts in the user networks support MLDv2.

Configure IPv6 PIM-SSM on each switch, so that the receiver hosts can receive VOD streams destined for an IPv6 multicast group in the IPv6 SSM group range **FF3E::/64** from a specific IPv6 multicast source.

Figure 92 Network diagram

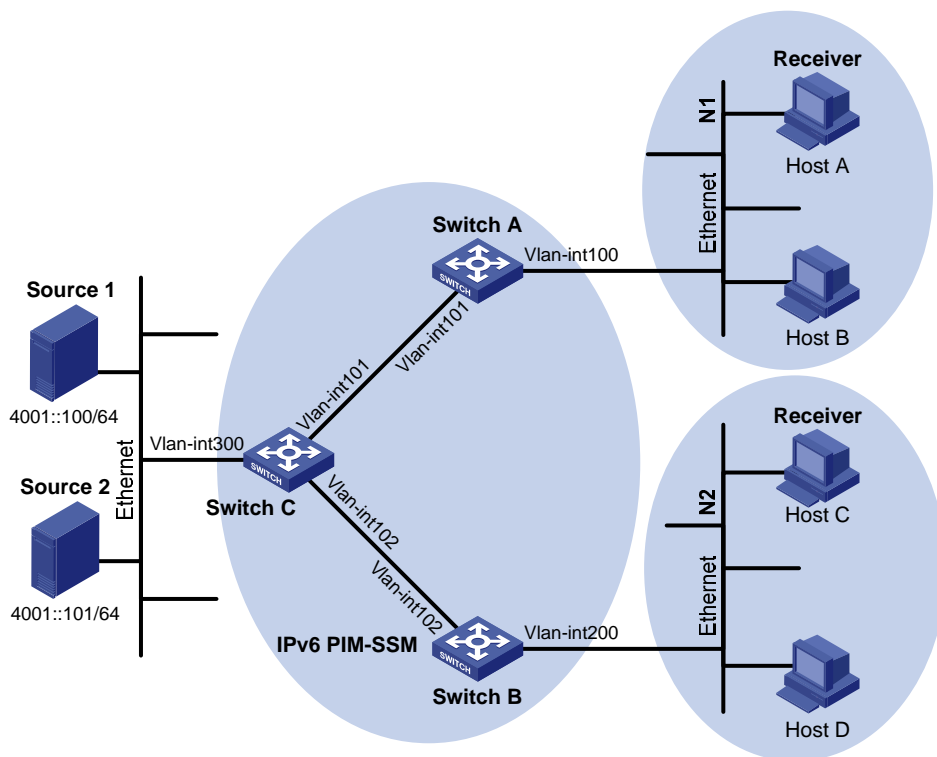


Table 6 Interface and IPv6 address assignment

Device	Interface	IPv6 address
Switch A	VLAN-interface 100	1001::1/64
Switch A	VLAN-interface 101	1002::1/64
Switch B	VLAN-interface 200	2001::1/64
Switch B	VLAN-interface 102	2002::1/64
Switch C	VLAN-interface 300	4001::1/64
Switch C	VLAN-interface 101	1002::2/64

Device	Interface	IPv6 address
Switch C	VLAN-interface 102	2002::2/64

Requirements analysis

To enable IPv6 PIM-SSM to provide services for IPv6 multicast groups in the range specified in the network requirements, you must specify this range on each Layer 3 switch.

In IPv6 SSM, the edge Layer 3 switch must get information about the specified multicast source when a host joins an IPv6 multicast group. To meet the requirement, you must enable MLDv2 on the edge switches that connect to the user networks.

Configuration restrictions and guidelines

When a member of an IPv6 multicast group in the IPv6 SSM group range sends an MLDv1 report message, the device does not trigger a (*, G) join. In this case, you can configure MLD SSM mappings, so that IPv6 PIM-SSM can provide services for hosts that support only MLDv1.

Configuration procedures

1. Enable IPv6 forwarding on the switches. (Details not shown.)
2. Assign an IPv6 address and prefix length to each interface according to [Table 6](#). (Details not shown.)
3. Configure OSPFv3 on the switches in the IPv6 PIM-SM domain. (Details not shown.)
4. Enable IPv6 multicast routing globally and configure IPv6 PIM-SSM:
 - # On Switch A, enable IPv6 multicast routing globally.

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
```

 - # On Switch A, enable IPv6 PIM-SM on each interface.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
[SwitchA-Vlan-interface101] quit
```

 - # Enable IPv6 multicast routing and IPv6 PIM-SM on Switch B and Switch C in the same way Switch A is configured. (Details not shown.)
5. Configure the IPv6 SSM group range:
 - # On Switch A, configure the IPv6 SSM group range to **FF3E::/64**.

```
[SwitchA] acl ipv6 number 2000
```



```
[SwitchA-acl6-basic-2000] rule permit source ff3e:: 64
[SwitchA-acl6-basic-2000] quit
[SwitchA] pim ipv6
[SwitchA-pim6] ssm-policy 2000
[SwitchA-pim6] quit
```

On Switch B and Switch C, configure the IPv6 SSM group ranges in the same way Switch A is configured. (Details not shown.)

6. Enable MLDv2 on the interfaces connected to the stub networks **N1** and **N2**:

On Switch A, enable MLDv2 on VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] mld version 2
[SwitchA-Vlan-interface100] quit
```

On Switch B, enable MLDv2 on VLAN-interface 200 in the same way Switch A is configured. (Details not shown.)

Verifying the configuration

1. Send an MLDv2 report from Host A to join the IPv6 multicast group **FF3E::101** and specify the IPv6 multicast source as **4001::100/64**. (Details not shown.)
2. Verify that correct (S, G) entries can be created on each switch. This configuration takes Switch A and Switch C as examples:

Display the PIM routing table on Switch A.

```
[SwitchA] display pim ipv6 routing-table
VPN-Instance: public net
Total 1 (S, G) entry
```

```
(4001::100, FF3E::101)
```

```
Protocol: pim-ssm, Flag:
UpTime: 00:00:11
Upstream interface: Vlan-interface101
    Upstream neighbor: FE80::223:89FF:FE5F:958C
    RPF prime neighbor: FE80::223:89FF:FE5F:958C
Downstream interface(s) information:
Total number of downstreams: 1
    1: Vlan-interface100
        Protocol: mld, UpTime: 00:00:11, Expires: 00:03:25
```

Display the PIM routing table on Switch C.

```
[SwitchC] display pim ipv6 routing-table
VPN-Instance: public net
Total 1 (S, G) entry
```

```
(4001::100, FF3E::101)
```

```
Protocol: pim-ssm, Flag: LOC
```

```

UpTime: 00:08:02
Upstream interface: Vlan-interface300
  Upstream neighbor: NULL
  RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 1
  1: Vlan-interface101
    Protocol: pim-ssm, UpTime: 00:08:02, Expires: 00:03:25

```

The output shows that Switch A builds an SPT toward the IPv6 multicast source. Switches on the SPT path (Switch A and Switch D) generate (S, G) entries.

Configuration files

- Switch A:

```

#
ipv6
#
multicast ipv6 routing-enable
#
acl ipv6 number 2000
  rule 0 permit source FF3E::/64
#
vlan 100 to 101
#
interface Vlan-interface100
  ipv6 address 1001::1/64
  ospfv3 1 area 0.0.0.0
  mld enable
  mld version 2
  pim ipv6 sm
#
interface Vlan-interface101
  ipv6 address 1002::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
ospfv3 1
  router-id 1.1.1.1
  area 0.0.0.0
#
pim ipv6
  ssm-policy 2000
#

```

- Switch B:

```

#
ipv6

```

```

#
multicast ipv6 routing-enable
#
acl ipv6 number 2000
  rule 0 permit source FF3E::/64
#
vlan 102
#
vlan 200
#
interface Vlan-interface102
  ipv6 address 2002::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
interface Vlan-interface200
  ipv6 address 2001::1/64
  ospfv3 1 area 0.0.0.0
  mld enable
  mld version 2
  pim ipv6 sm
#
ospfv3 1
  router-id 2.2.2.2
  area 0.0.0.0
#
pim ipv6
  ssm-policy 2000
#

```

- Switch C:

```

#
ipv6
#
multicast ipv6 routing-enable
#
acl ipv6 number 2000
  rule 0 permit source FF3E::/64
#
vlan 101 to 102
#
vlan 300
#
interface Vlan-interface101
  ipv6 address 1002::2/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
interface Vlan-interface102

```

```
ipv6 address 2002::2/64
ospfv3 1 area 0.0.0.0
pim ipv6 sm
#
interface Vlan-interface300
  ipv6 address 4001::1/64
  ospfv3 1 area 0.0.0.0
  pim ipv6 sm
#
ospfv3 1
  router-id 3.3.3.3
  area 0.0.0.0
#
pim ipv6
  ssm-policy 2000
#
```

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 5500 EI	Release 2220
HP 5500 SI	

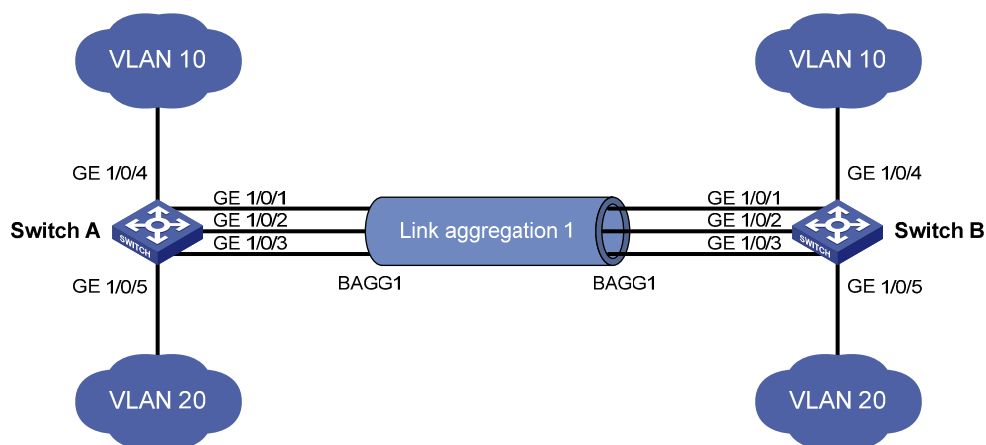
Network requirements

As shown in [Figure 93](#), 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 93 Network diagram



Requirements analysis

To enable traffic from VLAN 10 and VLAN 20 to pass through Layer 2 aggregate interface 1:

1. Configure the port link type of Layer 2 aggregate interface 1 as trunk.
2. Assign the 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 by source MAC address and destination MAC address, configure the link aggregation load sharing criteria in system view or aggregate interface 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 port view to display the class-two configurations of the port (including the port isolation configuration, QinQ configuration, VLAN configuration, and MAC address learning configuration).
 - b. If such configurations exist, use the **undo** forms of the corresponding commands to remove these configurations, so that the port uses the default class-two 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 use dynamic aggregation.
- A port with any of the following features configured or enabled cannot be assigned to a Layer 2 aggregation group: RRPP, MAC authentication, port security mode, IP source guard, 802.1X, or source interface of a portal-free rule.
- Only ports operating in bridge mode can be assigned to a Layer 2 link aggregation group.
- You can configure link aggregation load sharing in system view or aggregate interface view. This example uses configuring link aggregation load sharing in system view.

Configuration procedures

Configuring Switch A

Configure the link aggregation load sharing criteria as source MAC address and destination MAC address in system view.

```
<SwitchA> system-view
```

```
[SwitchA] link-aggregation load-sharing mode source-mac destination-mac
```

```

# Create VLAN 10, and assign port GigabitEthernet 1/0/4 to VLAN 10.
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/4
[SwitchA-vlan10] quit

# Create VLAN 20, and assign port GigabitEthernet 1/0/5 to VLAN 20.
[SwitchA] vlan 20
[SwitchA-vlan20] port gigabitethernet 1/0/5
[SwitchA-vlan20] quit

# Create Layer 2 aggregate interface 1. (Select 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 GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to aggregation group 1.
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/3] quit

# Configure Layer 2 aggregate interface 1 as a trunk port.
[SwitchA] interface bridge-aggregation 1
[SwitchA-Bridge-Aggregation1] port link-type trunk

# Assign the aggregate interface to VLANs 10 and 20.
[SwitchA-Bridge-Aggregation1] port trunk permit vlan 10 20
Please wait... Done.
Configuring GigabitEthernet 1/0/1... Done.
Configuring GigabitEthernet 1/0/2... Done.
Configuring GigabitEthernet 1/0/3... Done.
[SwitchA-Bridge-Aggregation1] quit

```

Configuring Switch B

Configure Switch B in the same way Switch A is configured.

Verifying the configuration

Use the **display link-aggregation verbose** command to display detailed information about the link aggregation groups to verify whether the configuration succeeds.

- Link aggregation configuration information when the static aggregation mode is used is as follows:

```
[SwitchA]display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
```

```
Aggregation Interface: Bridge-Aggregation1
```

```
Aggregation Mode: Static
```

```
Loadsharing Type: Shar
```

Port	Status	Priority	Oper-Key
GE1/0/1	S	32768	1
GE1/0/2	S	32768	1
GE1/0/3	S	32768	1

The output shows that all member ports in the local aggregation group are Selected. The Selected states of the local member ports are not affected by the Selected states of the peer member ports.

- Link aggregation configuration information when the dynamic aggregation mode is used is as follows:

```
[SwitchA]display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
```

```
Aggregation Interface: Bridge-Aggregation11
```

```
Aggregation Mode: Dynamic
```

```
Loadsharing Type: Shar
```

```
System ID: 0x8000, 000f-e234-5678
```

```
Local:
```

Port	Status	Priority	Oper-Key	Flag
GE1/0/1	S	32768	1	{ACDEF}
GE1/0/2	S	32768	1	{ACDEF}
GE1/0/3	S	32768	1	{ACDEF}

```
Remote:
```

Actor	Partner	Priority	Oper-Key	SystemID	Flag
GE1/0/1	14	32768	1	0x8000, 0000-fc00-7506	{ACDEF}
GE1/0/2	15	32768	1	0x8000, 0000-fc00-7506	{ACDEF}
GE1/0/3	16	32768	1	0x8000, 0000-fc00-7506	{ACDEF}

The output shows that the local member ports and the corresponding peer member ports are all Selected. Dynamic link aggregation ensures that each local member port and the corresponding peer member port have the same Selected state through exchanging LACPDU's between the two ends. The user data traffic can then be correctly forwarded.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```
#
link-aggregation load-sharing mode source-mac destination-mac
#
vlan 10
#
interface GigabitEthernet1/0/4
  port link-mode bridge
  port access vlan 10
#
vlan 20
#
interface GigabitEthernet1/0/5
  port link-mode bridge
  port access vlan 20
```

- Use the static aggregation mode:

```
#
interface Bridge-Aggregation1
  port link-type trunk
  port trunk permit vlan 10 20
```

- Use the dynamic aggregation mode:

```
#
interface Bridge-Aggregation1
  port link-type trunk
  port trunk permit vlan 10 20
  link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 10 20
  port link-aggregation group 1
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 10 20
  port link-aggregation group 1
#
interface GigabitEthernet1/0/3
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 10 20
```

```
port link-aggregation group 1
#
```

- 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 5500 EI	Release 2220
HP 5500 SI	

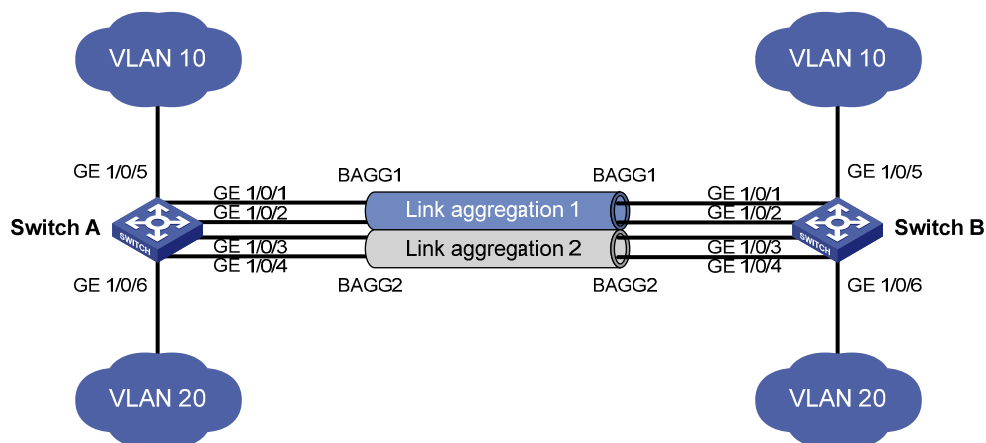
Network requirements

As shown in [Figure 94](#), 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 94 Network diagram



Requirements analysis

To configure different load sharing criteria for packets in different link aggregation groups, you must configure link aggregation load sharing criteria in Layer 2 aggregate interface view.

To enable packets from VLAN 10 to pass through aggregate interface 1, you must assign aggregate interface 1 to VLAN 10.

To enable packets from VLAN 20 to pass through aggregate interface 2, you must assign aggregate interface 2 to VLAN 20.

Configuration restrictions and guidelines

When you configure Layer 2 load sharing, follow these restrictions and guidelines:

- When you configure an aggregation group member port, the recommended configuration procedure is as follows:
 - a. Use the **display this** command in port view to display the class-two configurations of the port (including the port isolation configuration, QinQ configuration, VLAN configuration, and MAC address learning configuration).
 - b. If such configurations exist, use the **undo** forms of the corresponding commands to remove these configurations, so that the port uses the default class-two configurations.
 - c. Assign the port to an aggregation group.
- A port with any of the following features configured or enabled cannot be assigned to a Layer 2 aggregation group: RRPP, MAC authentication, port security mode, IP source guard, 802.1X, or source interface of a portal-free rule.
- Only ports operating in bridge mode can be assigned to a Layer 2 link aggregation group.

Configuration procedures

Configuring Switch A

```
# Create VLAN 10, and assign port GigabitEthernet 1/0/5 to VLAN 10.
```

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/5
[SwitchA-vlan10] quit
```

```
# Create VLAN 20, and assign port GigabitEthernet 1/0/6 to VLAN 20.
```

```
<SwitchA> system-view
[SwitchA] vlan 20
[SwitchA-vlan20] port gigabitethernet 1/0/6
[SwitchA-vlan20] quit
```

```
# Create layer 2 aggregate interface 1.
```

```

[SwitchA] interface bridge-aggregation 1

# Configure the link aggregation load sharing 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 GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 1.
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet 1/0/1] port link-aggregation group 1
[SwitchA-GigabitEthernet 1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet 1/0/2] port link-aggregation group 1
[SwitchA-GigabitEthernet 1/0/2] quit

# Assign Layer 2 aggregate interface 1 to VLAN 10.
[SwitchA] interface bridge-aggregation 1
[SwitchA-Bridge-Aggregation1] port access vlan 10
[SwitchA-Bridge-Aggregation1] quit

# Create layer 2 aggregate interface 2.
[SwitchA] interface bridge-aggregation 2

# Configure the link aggregation load sharing 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 GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to aggregation group 2.
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 2
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-aggregation group 2
[SwitchA-GigabitEthernet1/0/4] quit

# Assign layer 2 aggregate interface 2 to VLAN 20.
[SwitchA] interface bridge-aggregation 2
[SwitchA-Bridge-Aggregation2] port access vlan 20
[SwitchA-Bridge-Aggregation2] quit

```

Configuring Switch B

Configure Switch B in the same way Switch A is configured.

Verifying the configuration

```

# 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
GE1/0/1	S	32768	1
GE1/0/2	S	32768	1

```
Aggregation Interface: Bridge-Aggregation2
```

```
Aggregation Mode: Static
```

```
Loadsharing Type: Shar
```

Port	Status	Priority	Oper-Key
GE1/0/3	S	32768	2
GE1/0/4	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 the source MAC address.
- The link aggregation load sharing criteria for Layer 2 aggregate interface 2 is the destination MAC address.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```
#
vlan 10
#
```

```

interface GigabitEthernet1/0/5
port link-mode bridge
port access vlan 10
#
vlan 20
#
interface GigabitEthernet1/0/6
port link-mode bridge
port access vlan 10

```

- Configuration of aggregate interface 1:

```

#
interface Bridge-Aggregation1
port access vlan 10
link-aggregation load-sharing mode source-mac

```

- Configuration files of the member ports in aggregation group 1:

```

#
interface GigabitEthernet1/0/1
port link-mode bridge
port access vlan 10
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 10
port link-aggregation group 1

```

- Configuration of aggregate interface 2:

```

#
interface Bridge-Aggregation2
port access vlan 20
link-aggregation load-sharing mode destination-mac

```

- Configuration files of the member ports in aggregation group 2:

```

#
interface GigabitEthernet1/0/3
port link-mode bridge
port access vlan 20
port link-aggregation group 2
#
interface GigabitEthernet1/0/4
port link-mode bridge
port access vlan 20
port link-aggregation group 2

```

- Switch B:

The configuration file on Switch B is the same as the configuration file on Switch A.

Example: Configuring Layer 3 link aggregation

Applicable product matrix

Product series	Software Version
HP 5500 EI	Release 2220

Network requirements

Configure link aggregation and load sharing on Switch A and Switch B in the network shown in [Figure 95](#) to meet the following requirements:

- Ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A and Switch B preferentially become Selected ports.
- The packets between Switch A and Switch B are load-shared across only two member ports of the link aggregation group.
- The packets between Switch A and Switch B are load-shared by source IP address and destination IP address.

Figure 95 Network diagram



Requirements analysis

To make GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A and Switch B preferentially become Selected ports, assign higher aggregation priorities to the two ports. By default, the aggregation priority of a port is 32768. A smaller *port-priority* value in the **link-aggregation port-priority port-priority** command indicates a higher priority.

To load share packets across only two Selected ports of the link aggregation group, use the **link-aggregation selected-port maximum** command to configure the maximum number of Selected ports allowed in the aggregation group as 2.

Because the devices do not support configuring load sharing criteria in Layer 3 aggregate interface view, to configure the link aggregation load sharing for the Layer 3 aggregation group, you must configure the load sharing criteria in system view.

Configuration restrictions and guidelines

When you configure Layer 3 link aggregation, follow these restrictions and guidelines:

- By default, all Ethernet ports are operating in bridge mode as Layer 2 Ethernet ports. To assign an Ethernet port to a Layer 3 aggregation group, first use the **port link-mode route** command to configure the Ethernet port to operate in route mode as a Layer 3 Ethernet port.
- A port with any of the following features configured or enabled cannot be assigned to a Layer 3 aggregation group: IP address, DHCP client, BOOTP client, VRRP, and Portal.
- Executing the **link-aggregation selected-port maximum** command might cause some Selected ports in an aggregation group to be Unselected.

Configuration procedures

Configuring Switch A

Enter system view, and configure the global link aggregation load sharing criteria as source IP address and destination IP address.

```
<SwitchA> system-view  
[SwitchA] link-aggregation load-sharing mode source-ip destination-ip
```

Create Layer 3 aggregate interface 1. (Select one of the following methods as needed.)

- Use the static aggregation mode to create Layer 3 aggregate interface 1.
[SwitchA] interface route-aggregation 1
- Use the dynamic aggregation mode to create Layer 3 aggregate interface 1.
[SwitchA] interface route-aggregation 1
[SwitchA-Route-Aggregation1] link-aggregation mode dynamic

Assign an IP address 10.1.1.1 with a subnet mask 255.255.255.0 to Layer 3 aggregate interface 1.

```
[SwitchA-Route-Aggregation1] ip address 10.1.1.1 24
```

Configure the maximum number of Selected ports allowed in the aggregation group as 2.

```
[SwitchA-Route-Aggregation1] link-aggregation selected-port maximum 2  
[SwitchA-Route-Aggregation1] quit
```

Assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to aggregation group 1, and configure the aggregation priority as 100 for GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
[SwitchA] interface gigabitethernet 1/0/1  
[SwitchA-GigabitEthernet1/0/1] port link-mode route  
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 1  
[SwitchA-GigabitEthernet1/0/1] quit  
[SwitchA] interface gigabitethernet 1/0/2  
[SwitchA-GigabitEthernet1/0/2] port link-mode route  
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1  
[SwitchA-GigabitEthernet1/0/2] link-aggregation port-priority 100  
[SwitchA-GigabitEthernet1/0/2] quit  
[SwitchA] interface gigabitethernet 1/0/3
```



```
[SwitchA-GigabitEthernet1/0/3] port link-mode route
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/3] link-aggregation port-priority 100
[SwitchA-GigabitEthernet1/0/3] quit
```

Configuring Switch B

Configure Switch B in the same way Switch A is configured.

Verifying the configuration

Use the **display link-aggregation verbose** command to display detailed information about the link aggregation groups to verify whether the configuration succeeds.

- 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: Route-Aggregation1
```

```
Aggregation Mode: Static
```

```
Loadsharing Type: Shar
```

```
Port          Status  Priority  Oper-Key
```

```
-----
GE1/0/1       U       32768    1
GE1/0/2       S       100      1
GE1/0/3       S       100      1
```

- Link aggregation 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: Route-Aggregation2
```

```
Aggregation Mode: Dynamic
```

```
Loadsharing Type: Shar
```

```
System ID: 0x8000, 0000-fc00-7506
```

```
Local:
```

```
Port          Status  Priority  Oper-Key  Flag
```

```
-----
GE1/0/1       U       32768    1          {AC}
GE1/0/2       S       100      1          {ACDEF}
GE1/0/3       S       100      1          {ACDEF}
```

Remote:						
Actor	Partner	Priority	Oper-Key	SystemID	Flag	
GE1/0/1	122	32768	1	0x8000, 000f-e234-5678	{ACD}	
GE1/0/2	123	100	1	0x8000, 000f-e234-5678	{ACDEF}	
GE1/0/3	124	100	1	0x8000, 000f-e234-5678	{ACDEF}	

The output shows that only two ports in static aggregation group 1 can be Selected ports because the maximum number of Selected ports is limited. Because the aggregation priority of GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 is higher than that of GigabitEthernet 1/0/1, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 become Selected ports, and GigabitEthernet 1/0/1 becomes an Unselected port.

Configuration files

- Switch A:

```
#
link-aggregation load-sharing mode destination-ip source-ip
```

- Use the static aggregation mode:

```
#
interface Route-Aggregation1
link-aggregation selected-port maximum 2
ip address 10.1.1.1 255.255.255.0
```

- Use the dynamic aggregation mode:

```
#
interface Route-Aggregation2
link-aggregation mode dynamic
link-aggregation selected-port maximum 2
ip address 192.168.1.1 255.255.255.0
```

- Configuration files of the member ports:

```
#
interface GigabitEthernet1/0/1
port link-mode route
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
port link-mode route
link-aggregation port-priority 100
port link-aggregation group 1
#
interface GigabitEthernet1/0/3
port link-mode route
link-aggregation port-priority 100
port link-aggregation group 1
```

- Switch 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 5500 EI	Release 2220
HP 5500 SI	

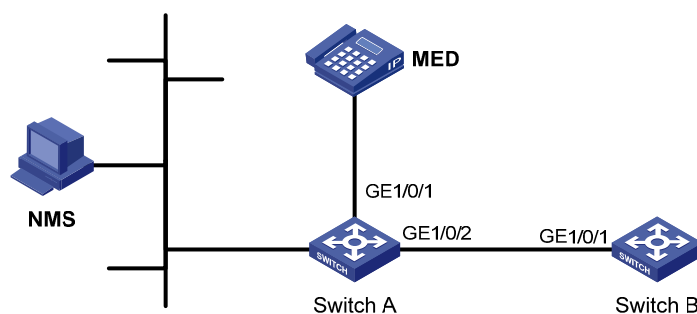
Network requirements

As shown in [Figure 96](#), the NMS and Switch A are located in the same Ethernet network.

Enable LLDP globally on Switch A and Switch B to monitor following:

- The link between Switch A and Switch B.
- The link between Switch A and the MED device on the NMS.

Figure 96 Network diagram



Configuration restrictions and guidelines

To view log information about neighbor changes on the terminal screen, make sure the following features are enabled:

- Use the **terminal monitor** command to enable the monitoring of system information on the terminal. By default, this feature is disabled.

- Use the **terminal logging** command to enable the display of log information on the terminal. By default, this feature is enabled.
- Use the **info-center enable** command to enable the information center. By default, this feature is enabled.

For more information about these features, see *Network Management and Monitoring Configuration Guide* in *HP 5500 EI & 5500 SI Series Switches Configuration Guides*.

Configuration procedures

1. Configure Switch A:

Enable LLDP globally. By default, LLDP is globally enabled.

```
<SwitchA> system-view
[SwitchA] lldp enable
```

Enable LLDP on GigabitEthernet 1/0/1, and set the LLDP operating mode to Rx. By default, LLDP is enabled on an interface.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] lldp enable
[SwitchA-GigabitEthernet1/0/1] lldp admin-status rx
[SwitchA-GigabitEthernet1/0/1] quit
```

Enable LLDP on GigabitEthernet 1/0/2, and set the LLDP operating mode to Rx. By default, LLDP is enabled on an interface.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] lldp enable
[SwitchA-GigabitEthernet1/0/2] lldp admin-status rx
[SwitchA-GigabitEthernet1/0/2] quit
```

2. Configure Switch B:

Enable LLDP globally. By default, LLDP is globally enabled.

```
<SwitchB> system-view
[SwitchB] lldp enable
```

Enable LLDP on GigabitEthernet 1/0/1, and set the LLDP operating mode to Tx. By default, LLDP is enabled on an interface.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] lldp enable
[SwitchB-GigabitEthernet1/0/1] lldp admin-status tx
[SwitchB-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display the global LLDP status and the LLDP status information of all ports on Switch A.

```
[SwitchA] display lldp status
Global status of LLDP : Enable
The current number of LLDP neighbors : 2
```

```
The current number of CDP neighbors : 0
LLDP neighbor information last changed time: 0 days,0 hours,4 minutes,40 seconds
Transmit interval          : 30s
Hold multiplier            : 4
Reinit delay               : 2s
Transmit delay             : 2s
Trap interval              : 5s
Fast start times           : 3
```

```
Port 1 [GigabitEthernet1/0/1]:
Port status of LLDP       : Enable
Admin status               : Rx_Only
Trap flag                  : No
Roll time                  : 0s
```

```
Number of neighbors       : 1
Number of MED neighbors   : 1
Number of CDP neighbors   : 0
Number of sent optional TLV : 0
Number of received unknown TLV : 0
```

```
Port 2 [GigabitEthernet1/0/2]:
Port status of LLDP       : Enable
Admin status               : Rx_Only
Trap flag                  : No
Roll time                  : 0s
```

```
Number of neighbors       : 1
Number of MED neighbors   : 0
Number of CDP neighbors   : 0
Number of sent optional TLV : 0
Number of received unknown TLV : 3
```

The output shows that:

- GigabitEthernet 1/0/1 of Switch A connects to an MED device.
- GigabitEthernet 1/0/2 of Switch A connects to a non-MED device.
- Both ports are operating in Rx mode.
- They can receive LLDPDUs, but they cannot send LLDPDUs.

Remove the link between Switch A and Switch B, and 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

Port 1 [GigabitEthernet1/0/1]:
Port status of LLDP    : Enable
Admin status           : Rx_Only
Trap flag              : No
Roll time              : 0s

Number of neighbors    : 1
Number of MED neighbors : 1
Number of CDP neighbors : 0
Number of sent optional TLV : 0
Number of received unknown TLV : 5

Port 2 [GigabitEthernet1/0/2]:
Port status of LLDP    : Enable
Admin status           : Rx_Only
Trap flag              : No
Roll time              : 0s

Number of neighbors    : 0
Number of MED neighbors : 0
Number of CDP neighbors : 0
Number of sent optional TLV : 0
Number of received unknown TLV : 0

```

The output shows that GigabitEthernet 1/0/2 of Switch A has no neighboring devices.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```

#
interface GigabitEthernet1/0/1
 port link-mode bridge
 lldp admin-status rx
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 lldp admin-status rx
#

```
- Switch B:

```

#
interface GigabitEthernet1/0/1

```

```
port link-mode bridge
lldp admin-status tx
#
```

Example: Configuring CDP-compatible LLDP

Applicable product matrix

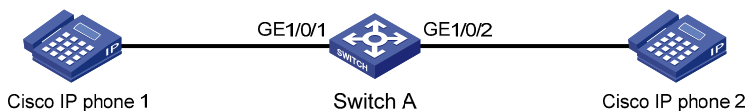
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 97](#), GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch A are each connected to a Cisco IP phone, which sends tagged voice traffic.

Configure voice VLAN 2 on Switch A. Enable CDP compatibility for LLDP on Switch A to allow the Cisco IP phones to automatically configure the voice VLAN. By confining their voice traffic to voice VLAN 2, the voice traffic is differentiated from other types of traffic.

Figure 97 Network diagram



Configuration restrictions and guidelines

When you configure CDP-compatible LLDP, follow these guidelines:

- To make CDP-compatible LLDP take effect on a port, you must enable CDP-compatible LLDP globally and configure the operating mode of CDP-compatible LLDP on the port as TxRx.
- The maximum TTL value that CDP allows is 255 seconds. To make CDP-compatible LLDP work correctly with Cisco IP phones, make sure the product of the TTL multiplier and the LLDPDU transmit interval is less than 255 seconds.

Configuration procedures

1. Configure a voice VLAN on Switch A:

```
# Create VLAN 2.
```



```

<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] quit

# Set the link type of GigabitEthernet 1/0/1 to trunk.
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk

# Enable voice VLAN on GigabitEthernet 1/0/1.
[SwitchA-GigabitEthernet1/0/1] voice vlan 2 enable
[SwitchA-GigabitEthernet1/0/1] quit

# Set the link type of GigabitEthernet 1/0/2 to trunk.
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk

# Enable voice VLAN on GigabitEthernet 1/0/2.
[SwitchA-GigabitEthernet1/0/2] voice vlan 2 enable
[SwitchA-GigabitEthernet1/0/2] quit

```

2. Configure CDP-compatible LLDP on Switch A:

```

# Enable both LLDP and CDP-compatible LLDP globally. By default, LLDP is globally enabled.
[SwitchA] lldp enable
[SwitchA] lldp compliance cdp

# Enable LLDP on GigabitEthernet 1/0/1. By default, LLDP is enabled on an interface.
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] lldp enable

# Configure LLDP to operate in TxRx mode on GigabitEthernet 1/0/1. The default LLDP operating mode is TxRx.
[SwitchA-GigabitEthernet1/0/1] lldp admin-status txrx

# Configure CDP-compatible LLDP to operate in TxRx mode on GigabitEthernet 1/0/1.
[SwitchA-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
[SwitchA-GigabitEthernet1/0/1] quit

# Enable LLDP on GigabitEthernet 1/0/2. By default, LLDP is enabled on an interface.
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] lldp enable

# Configure LLDP to operate in TxRx mode on GigabitEthernet 1/0/2. The default LLDP operating mode is TxRx.
[SwitchA-GigabitEthernet1/0/2] lldp admin-status txrx

# Configure CDP-compatible LLDP to operate in TxRx mode on GigabitEthernet 1/0/2.
[SwitchA-GigabitEthernet1/0/2] lldp compliance admin-status cdp txrx
[SwitchA-GigabitEthernet1/0/2] quit

```

Verifying the configuration

```

# Display the neighbor information on Switch A.
[SwitchA] display lldp neighbor-information

```

```
CDP neighbor-information of port 1[GigabitEthernet1/0/1]:
```

```
CDP neighbor index : 1
Chassis ID          : SEP00141CBCDBFE
Address             : 192.168.1.55
Port ID            : Port 1
Software version    : P0030301MFG2
Platform           : Cisco IP Phone 7960
Duplex             : Full
```

```
CDP neighbor-information of port 2[GigabitEthernet1/0/2]:
```

```
CDP neighbor index : 2
Chassis ID          : SEP00141CBCDBFF
Address             : 192.168.1.56
Port ID            : Port 1
Software version    : P0030301MFG2
Platform           : Cisco IP Phone 7960
Duplex             : Full
```

The sample output shows that:

- Switch A has discovered the IP phones connected to GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.
- Switch A has obtained the device information of these IP phones.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
lldp compliance cdp
#
vlan 2
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1
voice vlan 2 enable
lldp compliance admin-status cdp txrx
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 1
voice vlan 2 enable
lldp compliance admin-status cdp txrx
#
```

Login management configuration examples

This document provides examples for logging in to the switch through the console port, Telnet, and Web interface.

Example: Configuring console login

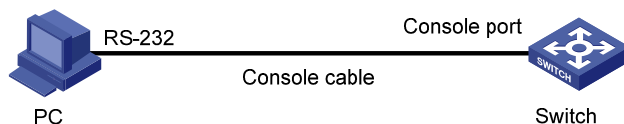
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 98](#), 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 98 Network diagram



Requirements analysis

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

- To log in to the switch, you only need 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, set the authentication mode to **scheme** for the console user interface and configure a local user.
- To enable a local user to log in through the console port and manage the switch, assign the terminal service and the privilege level 3 to the user. By default, a local user cannot use any service and can use only commands of level 0.

Configuration procedures

On the PC, run a terminal emulation program and create a connection, as shown in [Figure 99](#) and [Figure 100](#).

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, 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 99 Creating a connection

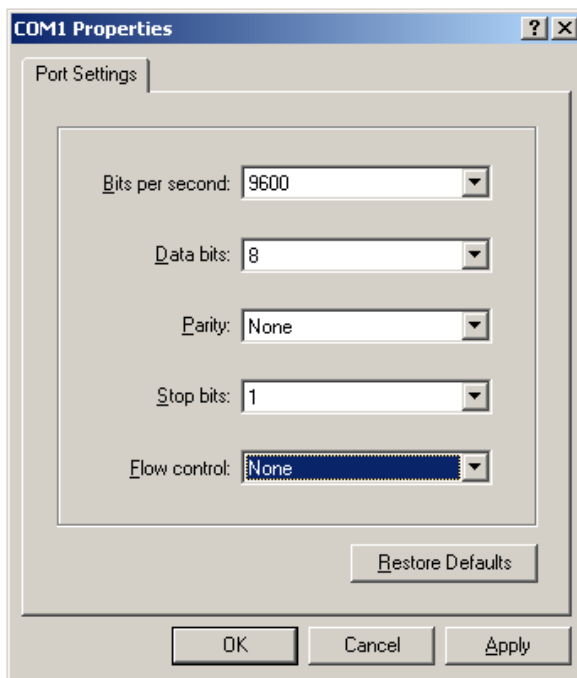


Figure 100 Specifying the connection port



Set communication parameters, as shown in [Figure 101](#).

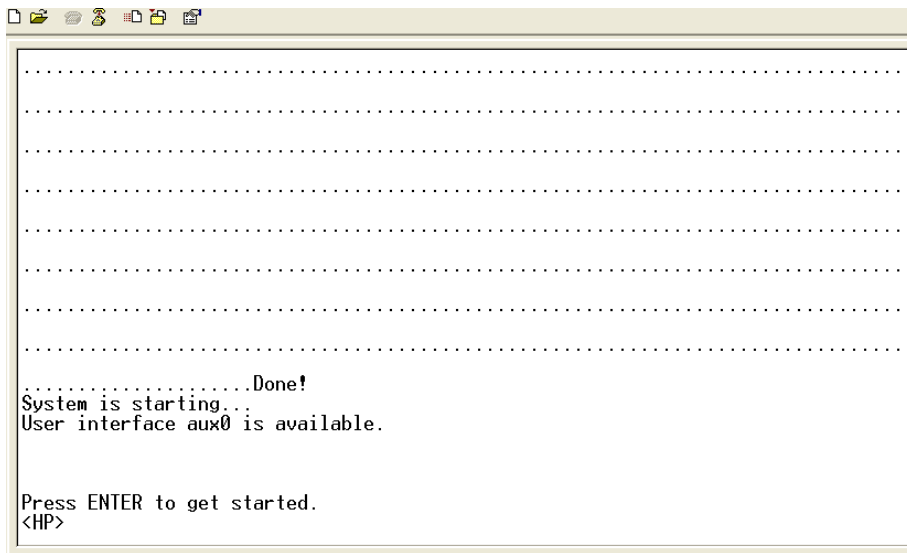
Figure 101 Setting communication parameters



Power on the switch.

After the switch starts up, the prompt <HP> appears, as shown in [Figure 102](#).

Figure 102 Login page



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 **Admin1234**.

```
[Sysname-luser-guest] password simple Admin1234)
```

Assign the terminal service and privilege level 3 to the user.

```
[Sysname-luser-guest] service-type terminal  
[Sysname-luser-guest] authorization-attribute level 3  
[Sysname-luser-guest] quit
```

Verifying the configuration

Terminate the current connection.

Log in to the switch through the console port again.

Verify that you must provide the configured username and password to log in.

Configuration files

```
#
local-user guest
  password cipher $c$3$wI+ls++f5LrYDLV7fR5DTEvRniz/+tHtbnYLBio=
  authorization-attribute level 3
  service-type terminal
#
user-interface aux 0
  authentication-mode scheme
```

Example: Configuring Telnet login

Applicable product matrix

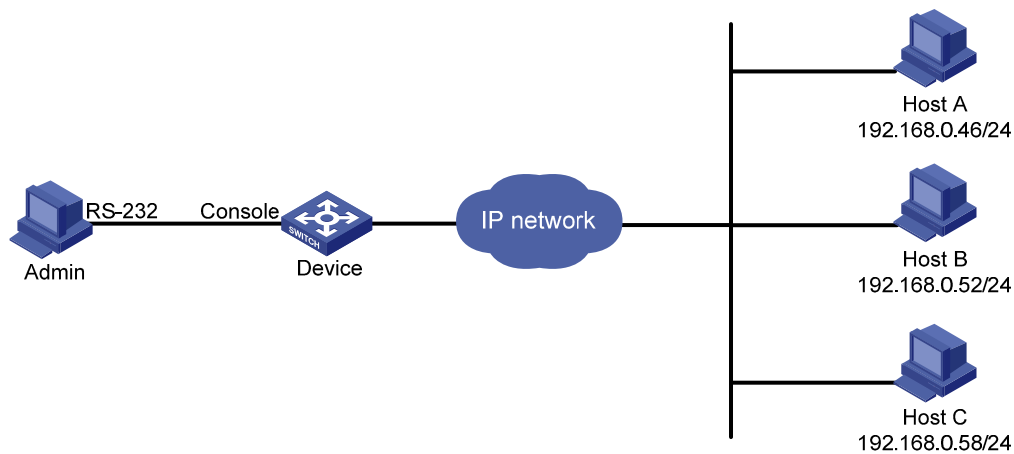
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 103](#), configure the switch to achieve the following goals:

- Only Host A and Host B can Telnet to the switch.
- Host A and Host B can Telnet to the switch without authentication and manage switch.

Figure 103 Network diagram



Requirements analysis

By default, Telnet login is disabled. To enable Telnet login, enable the Telnet server function.

The default privilege level of a Telnet user is 0. To enable Telnet users to manage the switch, assign the privilege level 3 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

# Set the privilege level to 3 for Telnet users.
[Sysname-ui-vty0-15] user privilege level 3

# Create basic ACL 2000.
[Sysname] acl number 2000
[Sysname-acl-basic-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] user-interface vty 0 15
[Sysname-ui-vty0-15] acl 2000 inbound
```

Verifying the configuration

```
# Verify that Host A and Host B can Telnet to the switch.
```

```
# Verify that Host C cannot Telnet to the switch.
```

Configuration files

```
#
telnet server enable
#
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
acl 2000 inbound
authentication-mode none
user privilege level 3
#

```

Example: Configuring Web login

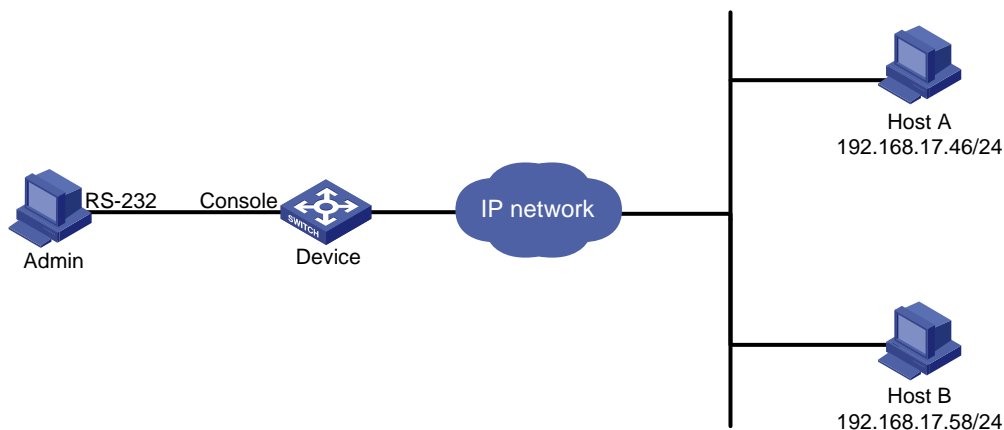
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 104](#), Host A and Host B can communicate with the switch at Layer 3. Configure the switch so only users on the subnet 192.168.17.0/24 can log in to the switch's Web interface to manage the switch.

Figure 104 Network diagram



Requirements analysis

By default, Web login is disabled. To enable Web login, log in to the switch through the console port and enable HTTP or HTTPS. In this example, HTTP is enabled.

To enable a Web user to manage the switch, assign the Web service and the privilege level 3 to the user.

Configuration procedures

```
# Enable the HTTP server function on the switch.
<Sysname> system-view
[Sysname] ip http enable

# Create a local user with the name admin and password admin.
[Sysname] local-user admin
[Sysname-luser-admin] password simple admin

# Assign the Web service and the privilege level 3 to the user.
[Sysname-luser-admin] service-type web
[Sysname-luser-admin] authorization-attribute level 3
[Sysname-luser-admin] quit

# Define a basic ACL.
[Sysname] acl number 2030
[Sysname-acl-basic-2030] rule 1 permit source 192.168.17.0 0.0.0.255

# Use the ACL to permit only users from 192.168.17.0/24 to access the switch.
[Sysname] ip http acl 2030
```

Verifying the configuration

```
# On Host A or Host B, launch a Web browser and enter http://192.168.17.52 in the address bar.

# Verify that the Web login page appears on the host.

# Enter the configured username admin and the password admin, and the verification code displayed on the login page. Verify that you are logged in to the Web interface.
```

Configuration files

```
#
ip http acl 2030
ip http enable
#
acl number 2030
rule 1 permit source 192.168.17.0 0.0.0.255
#
local-user admin
password cipher $c$3$jHCLjGzr9htQVvu6160mnfD+s73he3iO
authorization-attribute level 3
service-type web
#
```

MAC address table configuration examples

This chapter provides typical application scenarios and configuration examples for static, dynamic, and blackhole MAC address entries.

Example: Configuring the MAC address table

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

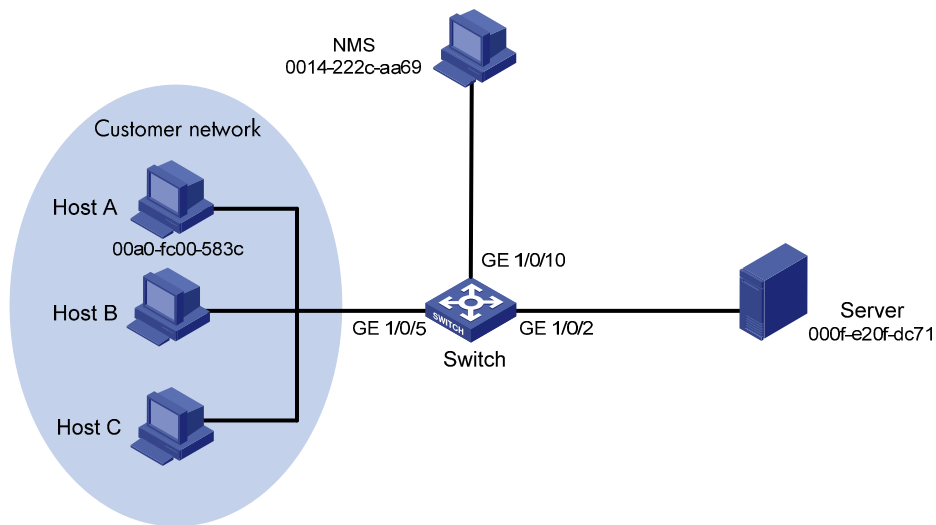
Network requirements

As shown in [Figure 105](#), the server, NMS, and the customer network forward traffic in VLAN 10.

Configure the MAC address table to meet the following requirements:

- The switch uses a static MAC address entry to only unicast the frames destined for the server.
- The switch uses a static MAC address entry to forward frames destined for the NMS.
- The interface connecting to the NMS provides access for only the NMS.
- The interface connecting to the customer network generates MAC address entries through learning source MAC addresses of incoming frames.
- The switch does not forward frames sourced from the host (Host A in this example) which launches attacks.

Figure 105 Network diagram



Requirements analysis

To allow the interface connecting to the NMS to provide access for only the NMS, set the MAC address learning limit to 0 on GigabitEthernet 1/0/10. As a result, the switch forwards only frames sourced from the NMS, and other hosts cannot communicate through the interface.

To prevent the switch from being attacked by a large amount of frames with different source MAC addresses from Host A, disable MAC address learning on GigabitEthernet 1/0/5.

Configuration restrictions and guidelines

The switch discards frames whose source or destination MAC address matches a blackhole MAC address entry.

Configuration procedures

Create VLAN 10, and assign interfaces GigabitEthernet 1/0/2, GigabitEthernet 1/0/5, and GigabitEthernet 1/0/10 to VLAN 10.

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] port GigabitEthernet1/0/2 GigabitEthernet1/0/5 GigabitEthernet1/0/10
[Switch-vlan10] quit
```

Create a static MAC address entry for the server MAC address on GigabitEthernet 1/0/2.

```
[Switch] mac-address static 000f-e20f-dc71 interface GigabitEthernet 1/0/2 vlan 10
```

Set the MAC address learning limit to 0 on GigabitEthernet 1/0/10.

```
[Switch] interface GigabitEthernet 1/0/10
```

```
[Switch-GigabitEthernet1/0/10] mac-address max-mac-count 0
# Configure a static MAC address entry for the NMS MAC address on the interface.
[Switch-GigabitEthernet1/0/10] mac-address static 0014-222c-aa69 vlan 10
# Disable MAC address learning on GigabitEthernet 1/0/5 when attacks are found on the interface.
Disabling MAC address learning can result in broadcast storms. To limit the size of broadcast traffic, set
the broadcast suppression threshold as 50% of the maximum interface rate.
[Switch] interface GigabitEthernet 1/0/5
[Switch-GigabitEthernet1/0/5] mac-address mac-learning disable
[Switch-GigabitEthernet1/0/5] broadcast-suppression 50
[Switch-GigabitEthernet1/0/5] quit
# After locating the attack source Host A, configure a blackhole MAC address entry for the Host A MAC
address.
[Switch] mac-address blackhole 00a0-fc00-583c vlan 10
# Enable MAC address learning on GigabitEthernet 1/0/5. Otherwise, broadcast storms might occur.
[Switch] interface GigabitEthernet 1/0/5
[Switch-GigabitEthernet1/0/5] undo mac-address mac-learning disable
[Switch-GigabitEthernet1/0/5] quit
# Disable broadcast suppression on GigabitEthernet 1/0/5.
[Switch-GigabitEthernet1/0/5] undo broadcast-suppression
```

Verifying the configuration

```
# Display the MAC address table configuration.
[Switch] display mac-address
MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME(s)
00a0-fc00-583c    10       Blackhole      N/A                 NOAGED
000f-e20f-dc71    10       Config static  GigabitEthernet1/0/2 NOAGED
0014-222c-aa69    10       Config static  GigabitEthernet1/0/10 NOAGED
00e0-fc5e-b1fb    10       Learned        GigabitEthernet1/0/5 AGING
00e0-fc55-f116    10       Learned        GigabitEthernet1/0/5 AGING
0000-fc00-7507    10       Learned        GigabitEthernet1/0/5 AGING
0023-8927-aff0    10       Learned        GigabitEthernet1/0/5 AGING
0023-8927-b003    10       Learned        GigabitEthernet1/0/5 AGING
--- 8 mac address(es) found ---
```

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
vlan 10
#
interface GigabitEthernet1/0/2
port link-mode bridge
```

```
port access vlan 10
mac-address static 000f-e20f-dc71 vlan 10
#
interface GigabitEthernet1/0/5
port link-mode bridge
port access vlan 10
#
interface GigabitEthernet1/0/10
port link-mode bridge
port access vlan 10
mac-address max-mac-count 0
mac-address static 0014-222c-aa69 vlan 10
#
mac-address blackhole 00a0-fc00-583c vlan 10
#
```

Example: Configuring MAC Information

Applicable product matrix

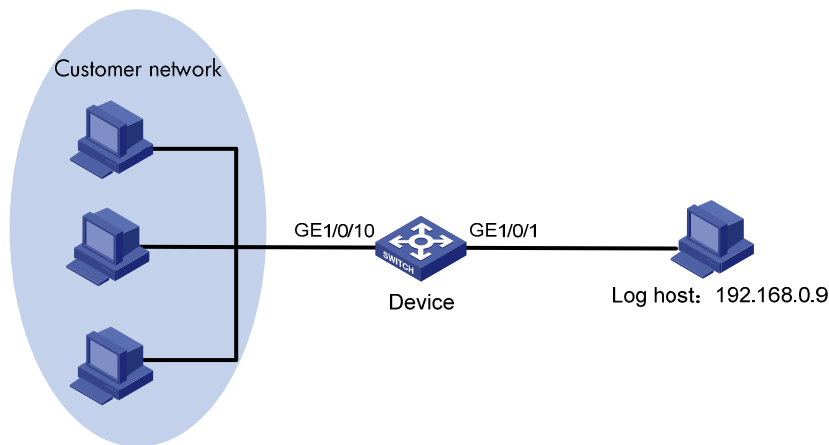
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 106](#), 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 106 Network diagram



Requirements analysis

To prevent syslog messages from being sent frequently, set the interval for sending syslog messages to 300 seconds.

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:
 - MAC addresses that are dynamically learned.
 - MAC addresses that pass MAC address authentication.
 - MAC addresses that pass 802.1X authentication.
 - MAC addresses that match the OUI addresses for voice VLANs.
 - Secure MAC addresses.
- The device does not record or send the following MAC addresses:
 - Blackhole MAC addresses.
 - Static MAC addresses.
 - Manually configured dynamic MAC addresses.
 - Multicast MAC addresses.
 - The local MAC address.
- Before configuring the device to send syslog messages to the log host, make sure the device and the log host can reach each other.

Configuration procedures

1. Configure MAC Information:

Enable MAC Information globally.

```
<Device> system-view
```

```
[Device] mac-address information enable
```

Configure the MAC Information mode as syslog.

```
[Device] mac-address information mode syslog
```

Enable MAC Information on GigabitEthernet 1/0/10.

```
[Device] interface gigabitethernet 1/0/10
```

```
[Device-GigabitEthernet1/0/10] mac-address information enable added
```

```
[Device-GigabitEthernet1/0/10] mac-address information enable deleted
```

```
[Device-GigabitEthernet1/0/10] quit
```

Set the interval for sending syslog messages to 300 seconds.

```
[Device] mac-address information interval 300
```

2. Configure the device to send syslog messages to the log host:

Enable the information center.

```
[Device] info-center enable
```

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 channel loghost log level informational state on
```

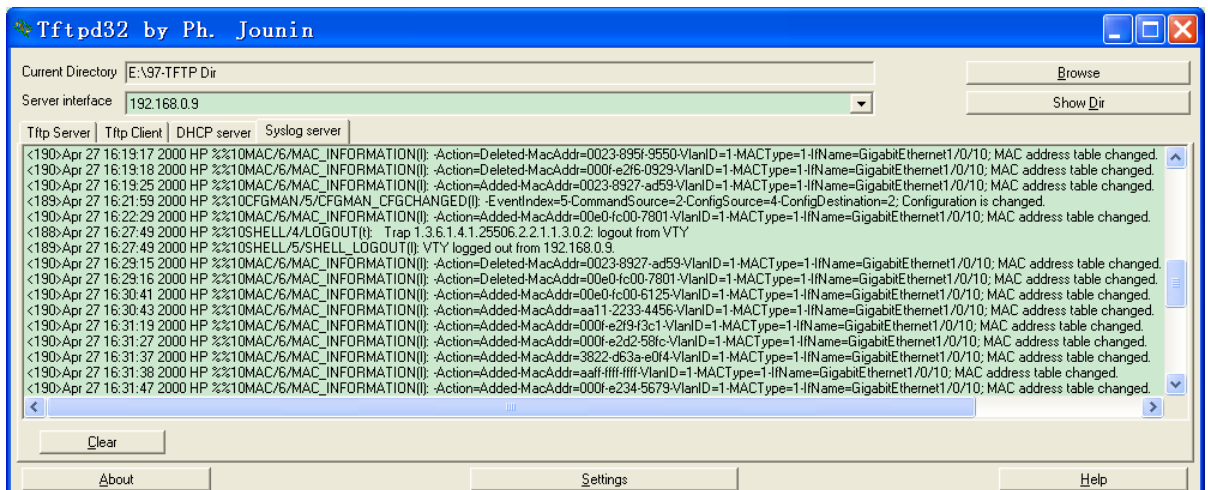
3. Run available applications that can receive log information on the log host.

Verifying the configuration

Display MAC Information messages on the log host to verify the configuration.

In this example, the **ftpd32** tool in the log host can receive log information. After you configure the above commands, the tool displays the log information, as shown in [Figure 107](#).

Figure 107 Log information



Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
mac-address information enable
mac-address information interval 300
mac-address information mode syslog
#
info-center enable
info-center source mac channel loghost log level informational state on
info-center loghost 192.168.0.9
#
interface GigabitEthernet1/0/10
port link-mode bridge
mac-address information enable added
mac-address information enable deleted
#
```

MAC authentication configuration examples

This chapter provides examples for configuring MAC authentication to control network access of users.

General restrictions and guidelines

MAC authentication is mutually exclusive with link aggregation and service loopback groups.

Example: Configuring local MAC authentication

Applicable product matrix

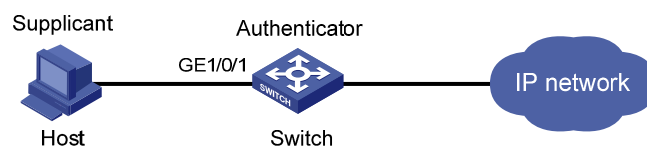
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 108](#):

- 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 must be hyphenated and in lower case.

Figure 108 Network diagram



Requirements analysis

The host is connected to GigabitEthernet 1/0/1 of the switch, so you must enable MAC authentication on the port.

To prevent continuous re-authentication of illegal MAC addresses, set MAC authentication timers.

Configuration restrictions and guidelines

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

- When you create a local user account, make sure the account 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 local 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
New local user added.
[Switch-luser-68-05-ca-06-55-7b] password simple 68-05-ca-06-55-7b
```

Enable LAN access service for the account.

```
[Switch-luser-68-05-ca-06-55-7b] service-type lan-access
[Switch-luser-68-05-ca-06-55-7b] quit
```

Configure ISP domain **aabbcc.net** to perform local authentication for LAN access users.

```
[Switch] domain aabbcc.net
[Switch-isp-aabbcc.net] authentication lan-access local
[Switch-isp-aabbcc.net] quit
```

Specify the ISP domain for MAC authentication.

```
[Switch] mac-authentication domain aabbcc.net
```

Set the MAC authentication offline detect timer. 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 must be hyphenated and in lower case.

```
[Switch] mac-authentication user-name-format mac-address with-hyphen lowercase
```

Enable MAC authentication on port GigabitEthernet 1/0/1.

```
[Switch] mac-authentication interface gigabitethernet 1/0/1
Mac-auth is enabled on port GigabitEthernet1/0/1.
```

Enable MAC authentication globally.

```
[Switch] mac-authentication
Mac-auth is enabled globally.
```

Verifying the configuration

```
# Display MAC authentication settings and statistics.
<Switch> display mac-authentication
MAC address authentication is enabled.
User name format is MAC address in lowercase, like xx-xx-xx-xx-xx-xx
Fixed username:mac
Fixed password:not configured
    Offline detect period is 180s
    Quiet period is 180s
    Server response timeout value is 100s
    The max allowed user number is 1024 per slot
    Current user number amounts to 1
    Current domain is aabbcc.net

Silent MAC User info:
          MAC Addr          From Port          Port Index

GigabitEthernet1/0/1 is link-up
MAC address authentication is enabled
Authenticate success: 1, failed: 364
Max number of on-line users is 256
Current online user number is 1
          MAC Addr          Authenticate State          Auth Index
          6805-ca06-557b    MAC_AUTHENTICATOR_SUCCESS    350
...

<Switch> display connection
Slot: 1
Index=350 , Username=68-05-ca-06-55-7b@aabbcc.net
IP=N/A
IPv6=N/A
MAC=6805-ca06-557b

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

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
mac-authentication
mac-authentication timer offline-detect 180
mac-authentication timer quiet 180
mac-authentication domain aabbcc.net
```

```

mac-authentication user-name-format mac-address with-hyphen
#
domain aabbcc.net
authentication lan-access local
access-limit disable
state active
idle-cut disable
self-service-url disable
#
local-user 68-05-ca-06-55-7b
password cipher $c$3$KEiYU/nrbJqmp75BldT4m99SzcSQ5Ro3sPRpTvUSd4aGL676
service-type lan-access
#
interface GigabitEthernet1/0/1
port link-mode bridge
mac-authentication
#

```

Example: Configuring RADIUS-based MAC authentication (MAC-based user account)

Applicable product matrix

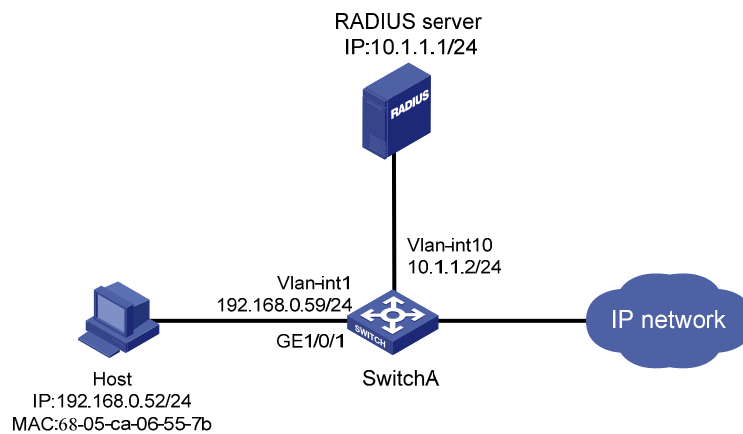
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 109](#):

- 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 must be hyphenated and in lower case.

Figure 109 Network diagram



Requirements analysis

The host is connected to GigabitEthernet 1/0/1 of the switch, so you must enable MAC authentication on the port.

To prevent continuous re-authentication of illegal MAC addresses, set MAC authentication timers.

Configuration restrictions and guidelines

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

- Enable MAC authentication globally only after you have configured the authentication-related parameters. Otherwise, users might fail to pass MAC authentication.
- When you create a user account on the RADIUS server, make sure the account has the same format as the one configured by the **mac-authentication user-name-format** command on the access device.
- The authentication port (UDP) used by RADIUS servers is 1812 according to standard RADIUS protocols. However, the port (UDP) is set to 1645 on an HP device that functions as the RADIUS authentication server. You must specify the authentication port as **1645** in the RADIUS scheme on the access device.

Configuration procedures

This example uses the HP 5500 HI switch as the RADIUS server. For more information about configuring the RADIUS server, see *HP 5500 HI Switch Series Security Configuration Guide*.

Configuring Switch A

Assign an IP address to each interface, as shown in [Figure 109](#). 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 abc
[SwitchA-radius-2000] user-name-format without-domain
[SwitchA-radius-2000] quit
```

Create ISP domain **domain2**, and apply the RADIUS scheme to the ISP domain for authentication and authorization of users.

```
[SwitchA] domain domain2
[SwitchA-isp-domain2] authentication lan-access radius-scheme 2000
[SwitchA-isp-domain2] authorization lan-access radius-scheme 2000
[SwitchA-isp-domain2] quit
```

Enable MAC authentication on GigabitEthernet 1/0/1.

```
[SwitchA] mac-authentication interface gigabitethernet 1/0/1
Mac-auth is enabled on port GigabitEthernet 1/0/1.
```

Specify the ISP domain for MAC authentication.

```
[SwitchA] mac-authentication domain domain2
```

Set the MAC authentication offline detect timer. 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 must be hyphenated and in lower case.

```
[SwitchA] mac-authentication user-name-format mac-address with-hyphen lowercase
```

Enable MAC authentication globally.

```
[SwitchA] mac-authentication
Mac-auth is enabled globally.
```

Configuring the RADIUS server

Create RADIUS user **68-05-ca-06-55-7b** (the host's MAC address) on the RADIUS server, and enter RADIUS-server user view.

```
<SwitchB> system-view
[SwitchB] radius-server user 68-05-ca-06-55-7b
```

Set the password to **123456** in plain text for RADIUS user **68-05-ca-06-55-7b**.

```
[SwitchB-rdsuser-68-05-ca-06-55-7b] password simple 123456
[SwitchB-rdsuser-68-05-ca-06-55-7b] quit
```

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

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

Verifying the configuration

Display MAC authentication settings and statistics.

```
<SwitchA> display mac-authentication
```

```
MAC address authentication is enabled.
```

```
User name format is MAC address in lowercase, like xx-xx-xx-xx-xx-xx
```

```
Fixed username:mac
```

```
Fixed password:not configured
```

```
    Offline detect period is 180s
```

```
    Quiet period is 180s.
```

```
    Server response timeout value is 100s
```

```
    The max allowed user number is 1024 per slot
```

```
    Current user number amounts to 1
```

```
    Current domain is domain2
```

```
Silent Mac User info:
```

MAC Addr	From Port	Port Index
----------	-----------	------------

```
Gigabitethernet1/0/1 is link-up
```

```
MAC address authentication is enabled
```

```
Authenticate success: 1, failed: 0
```

```
Max number of on-line users is 256
```

```
Current online user number is 1
```

MAC Addr	Authenticate State	Auth Index
6805-ca06-557b	MAC_AUTHENTICATOR_SUCCESS	0

```
...
```

```
<SwitchA> display connection
```

```
Slot: 1
```

```
Index=0 ,Username=68-05-ca-06-55-7b@domain2
```

```
IP=N/A
```

```
Ipv6=N/A
```

```
MAC=6805-ca06-557b
```

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

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

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```
#
```

```
mac-authentication
```



```

mac-authentication timer offline-detect 180
mac-authentication timer quiet 180
mac-authentication domain domain2
mac-authentication user-name-format mac-address with-hyphen
#
radius scheme 2000
  primary authentication 10.1.1.1 1645 key cipher $c$3$eYcHkFXUguZArZkXiCkrPABwQ0
+E6g==
  user-name-format without-domain
#
domain domain2
  authentication lan-access radius-scheme 2000
  authorization lan-access radius-scheme 2000
  access-limit disable
  state active
  idle-cut disable
  self-service-url disable
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  mac-authentication
#

```

- RADIUS server:

```

#
radius-server client-ip 10.1.1.2 key cipher $c$3$qz/+3koDvrIbRqm1Ghf6a10hS4fLFQ
==
#
radius-server user 68-05-ca-06-55-7b
  password cipher $c$3$Xv+yKBbrO2y10iVyWZfuRJyhm0ZNJkGU/REI5+GZSfJ7vcky
#

```

Example: Configuring RADIUS-based MAC authentication (shared user account)

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

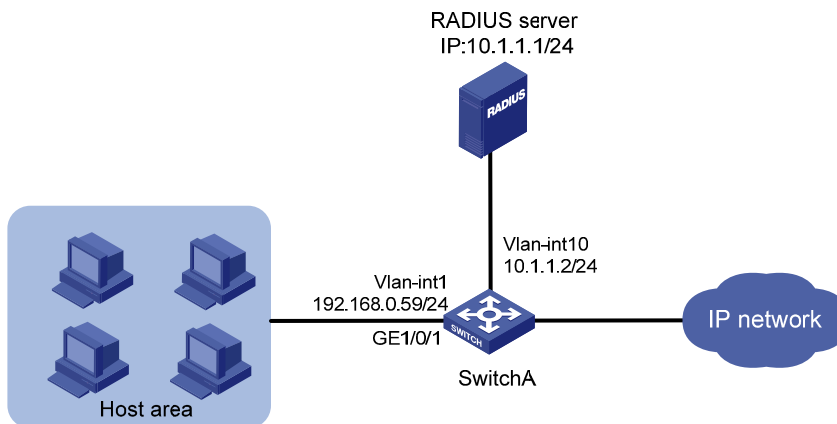
Network requirements

As shown in [Figure 110](#):

- 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**.

The hosts are in a secure network.

Figure 110 Network diagram



Requirements analysis

The host is connected to GigabitEthernet 1/0/1 of the switch, so you must enable MAC authentication on the port.

To prevent continuous re-authentication of illegal MAC addresses, set MAC authentication timers.

Configuration restrictions and guidelines

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

- Enable MAC authentication globally only after you have configured the authentication-related parameters. Otherwise, users might fail to pass MAC authentication.
- When you create a user account on the RADIUS server, make sure the account has the same format as the one configured by the **mac-authentication user-name-format** command on the access device.
- The authentication port (UDP) used by RADIUS servers is 1812 according to standard RADIUS protocols. However, the port (UDP) is set to 1645 on an HP device that functions as the RADIUS authentication server. You must specify the authentication port as **1645** in the RADIUS scheme on the access device.

Configuration procedures

This example uses the HP 5500 HI switch as the RADIUS server. For more information about configuring the RADIUS server, see *HP 5500 HI Switch Series Security Configuration Guide*.

Configuring Switch A

Assign an IP address to each interface, as shown in [Figure 110](#). 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 abc
[SwitchA-radius-2000] user-name-format without-domain
[SwitchA-radius-2000] quit
```

Create ISP domain **domain1**, and apply the RADIUS scheme to the ISP domain for authentication and authorization of users.

```
[SwitchA] domain domain1
[SwitchA-isp-domain1] authentication lan-access radius-scheme 2000
[SwitchA-isp-domain1] authorization lan-access radius-scheme 2000
[SwitchA-isp-domain1] quit
```

Enable MAC authentication on GigabitEthernet 1/0/1.

```
[SwitchA] mac-authentication interface gigabitethernet 1/0/1
Mac-auth is enabled on port GigabitEthernet1/0/1.
```

Specify the ISP domain for MAC authentication.

```
[SwitchA] mac-authentication domain domain1
```

Set the MAC authentication offline detect timer. 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
```

Specify username **aaa** and password **123456** in plain text for the account shared by MAC authentication users.

```
[SwitchA] mac-authentication user-name-format fixed account aaa password simple 123456
```

Enable MAC authentication globally.

```
[SwitchA] mac-authentication
Mac-auth is enabled globally.
```

Configuring the RADIUS server

Create RADIUS user **aaa** on the RADIUS server, and enter RADIUS-server user view.

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

```
[SwitchB] radius-server user aaa

# Set the password to 123456 in plain text for RADIUS user aaa.
[SwitchB-rdsuser-aaa] password simple 123456
[SwitchB-rdsuser-aaa] quit

# Specify RADIUS client 10.1.1.2 and set the shared key to abc in plain text.
[SwitchB] radius-server client-ip 10.1.1.2 key simple abc
```

Verifying the configuration

Display MAC authentication settings and statistics on Switch A.

```
<SwitchA> display mac-authentication
MAC address authentication is enabled.
User name format is fixed account
Fixed username:aaa
Fixed password:*****
    Offline detect period is 180s
    Quiet period is 180s.
    Server response timeout value is 100s
    The max allowed user number is 1024 per slot
    Current user number amounts to 4
    Current domain is domain1

Silent Mac User info:
      MAC Addr           From Port           Port Index

Gigabitethernet1/0/1 is link-up
MAC address authentication is enabled
Authenticate success: 4, failed: 0
Max number of on-line users is 256
Current online user number is 4
      MAC Addr           Authenticate State   Auth Index
      6805-ca06-557b     MAC_AUTHENTICATOR_SUCCESS  0
      6805-ca00-8a11     MAC_AUTHENTICATOR_SUCCESS  1
      6805-ca00-6677     MAC_AUTHENTICATOR_SUCCESS  2
      6805-ca02-1122     MAC_AUTHENTICATOR_SUCCESS  3

...

<SwitchA> display connection
Slot: 1
Index=0 ,Username=aaa@domain1
IP=N/A
Ipv6=N/A
MAC=6805-ca06-557b
Index=1 ,Username=aaa@domain1
IP=N/A
```

```

Ipv6=N/A
MAC=6805-ca00-8a11
Index=2 ,Username=aaa@domain1
IP=N/A
Ipv6=N/A
MAC=6805-ca00-6677
Index=3 ,Username=aaa@domain1
IP=N/A
Ipv6=N/A
MAC=6805-ca02-1122

```

Total 4 connection(s) matched on slot 1.

Total 4 connection(s) matched.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```

#
mac-authentication
  mac-authentication timer offline-detect 180
  mac-authentication timer quiet 180
  mac-authentication domain domain1
  mac-authentication user-name-format fixed account aaa password cipher $c$3$6DXU
G/ZZMl7AbkMpJEo2uoni19WCI0nJGw
#
radius scheme 2000
  primary authentication 10.1.1.1 1645 key cipher $c$3$eYcHkFXUguZArZkXiCkrPABwQ0
+E6g
  user-name-format without-domain
#
domain domain1
  authentication lan-access radius-scheme 2000
  authorization lan-access radius-scheme 2000
  access-limit disable
  state active
  idle-cut disable
  self-service-url disable
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  mac-authentication
#

```

- RADIUS server:

```

#
radius-server client-ip 10.1.1.2 key cipher $c$3$qz/+3koDvrIbRqm1Ghf6a10hS4fLFQ
==

```

```
#
radius-server user aaa
password cipher $c$3$Xv+yKBbrO2y10iVyWZfuRJyhm0ZNJkGU/REI5+GZSfJ7vcky
#
```

Example: Configuring MAC authentication with ACL assignment

Applicable product matrix

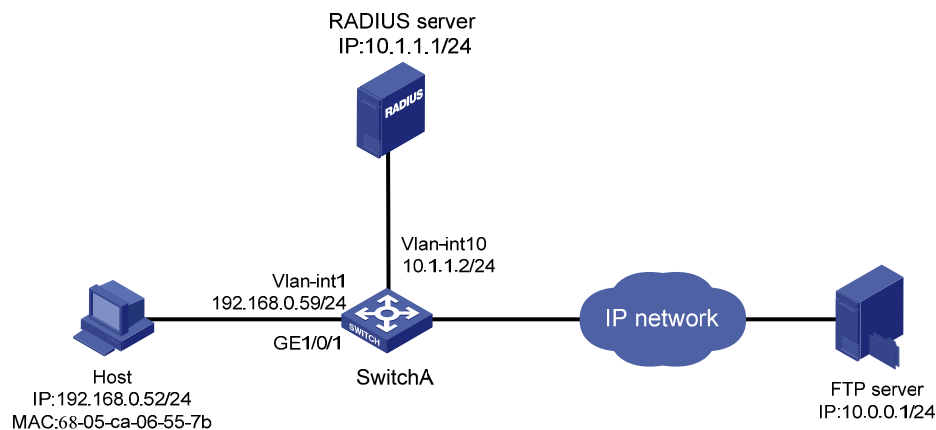
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

Network requirements

As shown in [Figure 111](#):

- Configure RADIUS-based MAC authentication on the switch to control Internet access of users.
- Apply an ACL to authenticated users to make sure these users can access the Internet but not the FTP server at 10.0.0.1.
- Use MAC-based user accounts for MAC authentication users. The MAC addresses must be hyphenated and in lower case.

Figure 111 Network diagram



Requirements analysis

The host is connected to GigabitEthernet 1/0/1 of the switch, so you must enable MAC authentication on the port.

To prevent continuous re-authentication of illegal MAC addresses, set MAC authentication timers.

To identify valid users, you must add a user account for each user on the RADIUS server.

To make the switch implement ACL assignment, you must configure an ACL on the switch and specify the ACL as the authorization ACL.

Configuration restrictions and guidelines

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

- Enable MAC authentication globally only after you have configured the authentication-related parameters. Otherwise, users might fail to pass MAC authentication.
- When you create a user account on the RADIUS server, make sure the account has the same format as the one configured by the **mac-authentication user-name-format** command on the access device.
- The authentication port (UDP) used by RADIUS servers is 1812 according to standard RADIUS protocols. However, the port (UDP) is set to 1645 on an HP device that functions as the RADIUS authentication server. You must specify the authentication port as **1645** in the RADIUS scheme on the access device.

Configuration procedures

This example uses the HP 5500 HI switch as the RADIUS server. For more information about configuring the RADIUS server, see *HP 5500 HI Switch Series Security Configuration Guide*.

Configuring Switch A

Assign an IP address to each interface, as shown in [Figure 111](#). 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 abc
[SwitchA-radius-2000] user-name-format without-domain
[SwitchA-radius-2000] quit
```

Create ISP domain **domain1**, and apply the RADIUS scheme to the ISP domain for authentication and authorization of users.

```

[SwitchA] domain domain1
[SwitchA-isp-domain1] authentication lan-access radius-scheme 2000
[SwitchA-isp-domain1] authorization lan-access radius-scheme 2000
[SwitchA-isp-domain1] quit

# Configure ACL 3000 to deny packets destined for 10.0.0.1.
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0
[SwitchA-acl-adv-3000] quit

# Enable MAC authentication on GigabitEthernet 1/0/1.
[SwitchA] mac-authentication interface gigabitethernet 1/0/1
Mac-auth is enabled on port GigabitEthernet1/0/1.

# Specify the ISP domain for MAC authentication.
[SwitchA] mac-authentication domain domain1

# Set the MAC authentication timers.
[SwitchA] mac-authentication timer offline-detect 180
[SwitchA] mac-authentication timer quiet 180

# Configure the switch to use MAC-based user accounts. The MAC addresses must be hyphenated and
in lower case.
[SwitchA] mac-authentication user-name-format mac-address with-hyphen lowercase

# Enable MAC authentication globally.
[SwitchA] mac-authentication
Mac-auth is enabled globally.

```

Configuring the RADIUS server

```

# Add a user account with 68-05-ca-06-55-7b (the host's MAC address) as the username on the RADIUS
server, and enter RADIUS-server user view.
<SwitchB> system-view
[SwitchB] radius-server user 68-05-ca-06-55-7b

# Set the password to 123456 in plain text for the user account.
[SwitchB-rdsuser-68-05-ca-06-55-7b] password simple 123456

# Specify ACL 3000 as the authorization ACL for the user account.
[SwitchB-rdsuser-68-05-ca-06-55-7b] authorization-attribute acl 3000
[SwitchB-rdsuser-68-05-ca-06-55-7b] quit

# Specify RADIUS client 10.1.1.2 and set the shared key to abc in plain text.
[SwitchB] radius-server client-ip 10.1.1.2 key simple abc

```

Verifying the configuration

```

# After the host passes authentication, use the display connection command on Switch A to display
online user information.
<SwitchA> display connection
Slot: 1

```



```
Index=0 ,Username=68-05-ca-06-55-7b@domain1
IP=N/A
Ipv6=N/A
MAC=6805-ca06-557b
```

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

Ping the FTP server from the host. The output shows that the ACL 3000 has been assigned to port GigabitEthernet 1/0/1 to deny access to the FTP server.

```
C:\>ping 10.0.0.1
```

```
Pinging 10.0.0.1 with 32 bytes of data:
```

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

```
Ping statistics for 10.0.0.1:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

```
C:\>
```

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```
#
mac-authentication
  mac-authentication timer offline-detect 180
  mac-authentication timer quiet 180
  mac-authentication domain domain2
  mac-authentication user-name-format mac-address with-hyphen
#
acl number 3000
  rule 0 deny ip destination 10.0.0.1 0
#
radius scheme 2000
  primary authentication 10.1.1.1 1645 key cipher $c$3$eYcHkFXUguZArZkXiCkrPABwQ0
+E6g==
  user-name-format without-domain
#
domain domain1
  authentication lan-access radius-scheme 2000
  authorization lan-access radius-scheme 2000
  access-limit disable
```

```
state active
idle-cut disable
self-service-url disable
#
interface GigabitEthernet1/0/1
port link-mode bridge
mac-authentication
#
```

- RADIUS server:

```
#
radius-server client-ip 10.1.1.2 key cipher $c$3$qz/+3koDvrIbRqm1Ghf6a10hS4fLFQ
==
#
radius-server user 68-05-ca-06-55-7b
password cipher $c$3$Xv+yKBbrO2y10iVyWZfuRjyhm0ZnJkGU/REI5+GZSfJ7vcky
authorization-attribute acl 3000
#
```

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 5500 EI	Release 2220

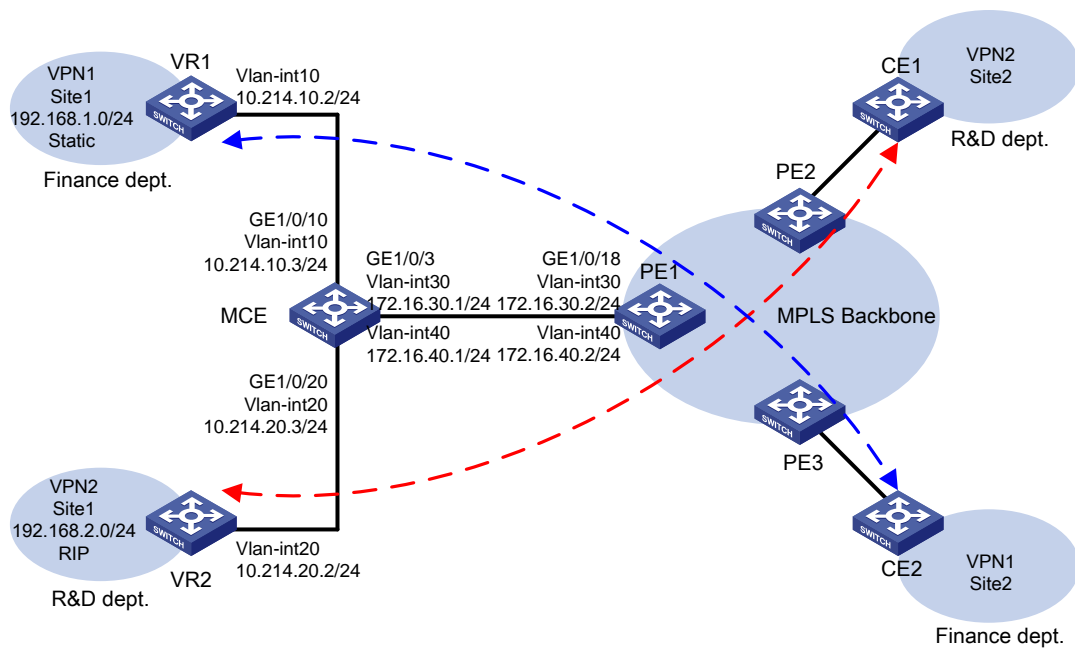
Network requirements

As shown in [Figure 112](#), an enterprise has two MPLS L3VPNs connected over an MPLS backbone. VPN 1 for the finance department uses static 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.
- The MCE exchanges routes with PE1 through OSPF.
- VPN sites can exchange VPN routes through PEs.

Figure 112 Network diagram



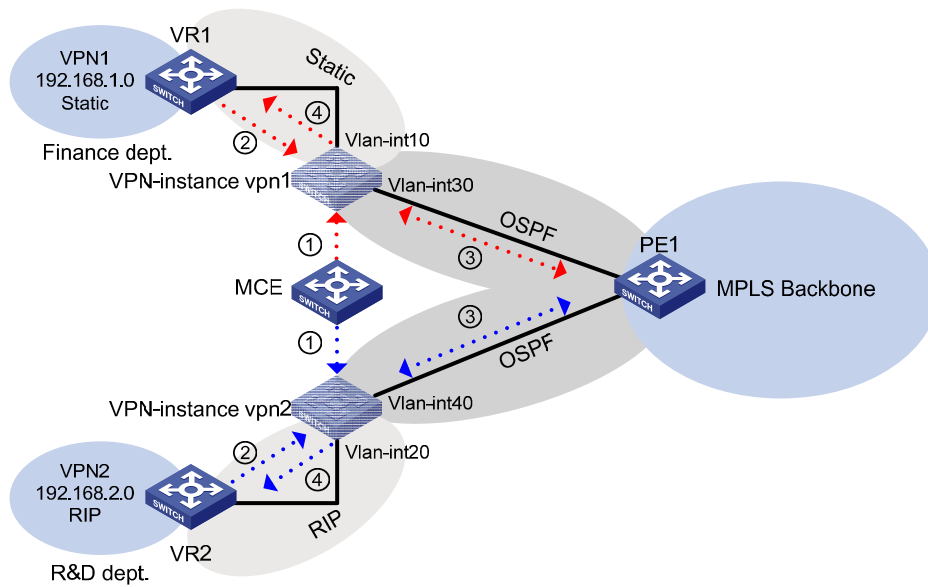
Requirements analysis

To isolate VPNs, 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 113 shows the order in which the MCE processes routing information for each VPN.

For the VPN sites to exchange VPN routes, configure the VPN instances on the MCE to perform the following:

- 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 113 Network diagram



Configuration restrictions and guidelines

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

- The **ip binding vpn-instance** command removes the IP address of the bound interface. After you execute the **ip binding vpn-instance** command on an interface, you must re-configure an IP address for that 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

This example only shows the configurations on the MCE and the connected devices VR1, VR2 and PE1.

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, add GigabitEthernet 1/0/10 to VLAN 10, and create VLAN-interface 10.
[MCE] vlan 10
[MCE-vlan10] port GigabitEthernet 1/0/10
[MCE-vlan10] quit
[MCE] interface Vlan-interface 10

# Bind VLAN-interface 10 to VPN instance vpn1, and configure IP address 10.214.10.3/24 for the VLAN
interface.
[MCE-Vlan-interface10] ip binding vpn-instance vpn1
[MCE-Vlan-interface10] ip address 10.214.10.3 24
[MCE-Vlan-interface10] quit

# Create VLAN 20, and add GigabitEthernet 1/0/20 to VLAN 20.
[MCE] vlan 20
[MCE-vlan20] port 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 VLAN-interface 20.
[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 GigabitEthernet 1/0/3 to the two VLANs.
[MCE] interface GigabitEthernet 1/0/3
[MCE-GigabitEthernet1/0/3] port link-type trunk
[MCE-GigabitEthernet1/0/3] port trunk permit vlan 30 40
[MCE-GigabitEthernet1/0/3] quit

# Create VLAN-interface 30, and bind VLAN-interface 30 to VPN instance vpn1.
[MCE] interface Vlan-interface 30
[MCE-Vlan-interface30] ip binding vpn-instance vpn1

# Configure IP address 172.16.30.1/24 for VLAN-interface 30.
[MCE-Vlan-interface30] ip address 172.16.30.1 24
[MCE-Vlan-interface30] quit

# Create VLAN-interface 40, and bind VLAN-interface 40 to VPN instance vpn2.
[MCE] interface Vlan-interface 40
[MCE-Vlan-interface40] ip binding vpn-instance vpn2

# Configure IP address 172.16.40.1/24 for VLAN-interface 40.

```

```
[MCE-Vlan-interface40] ip address 172.16.40.1 24
[MCE-Vlan-interface40] quit
```

On PE1, configure the VPN instances and RDs, and bind VPN instances to the interface that connects to the MCE. (Details not shown.)

HP recommends configuring 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 VR1, configure IP address 192.168.1.1/24 for the interface that connects to VPN 1 site 1, and configure VLAN settings. (Details not shown.)

On VR1, 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, and 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
Routing Tables: 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 VR2, configure IP address 10.214.20.2/24 for the interface that connects to the MCE. (Details not shown.)

On VR2, 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
```

```
Routing Tables: vpn2
      Destinations : 5          Routes : 5
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, and add GigabitEthernet1/0/18 to the two VLANs.

```
<PE1> system-view
[PE1] vlan 30
[PE1-vlan30] quit
[PE1] vlan 40
[PE1-vlan40] quit
[PE1] interface GigabitEthernet 1/0/18
[PE1-GigabitEthernet1/0/18] port link-type trunk
[PE1-GigabitEthernet1/0/18] port trunk permit vlan 30 40
[PE1-GigabitEthernet1/0/18] undo port trunk permit vlan 1
[PE1-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 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
```

Configure interface loopback 0 and bind it to VPN instance **vpn1** on the MCE and PE.

```
[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 for 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 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 for 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 for 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
Routing Tables: 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
display ip routing-table vpn-instance vpn2
Routing Tables: 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 GigabitEthernet1/0/3
  port link-type trunk
```

```

port trunk permit vlan 1 30 40
#
interface GigabitEthernet1/0/10
port access vlan 10
#
interface 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 GigabitEthernet1/0/18
 port link-mode bridge
 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 5500 EI	Release 2220

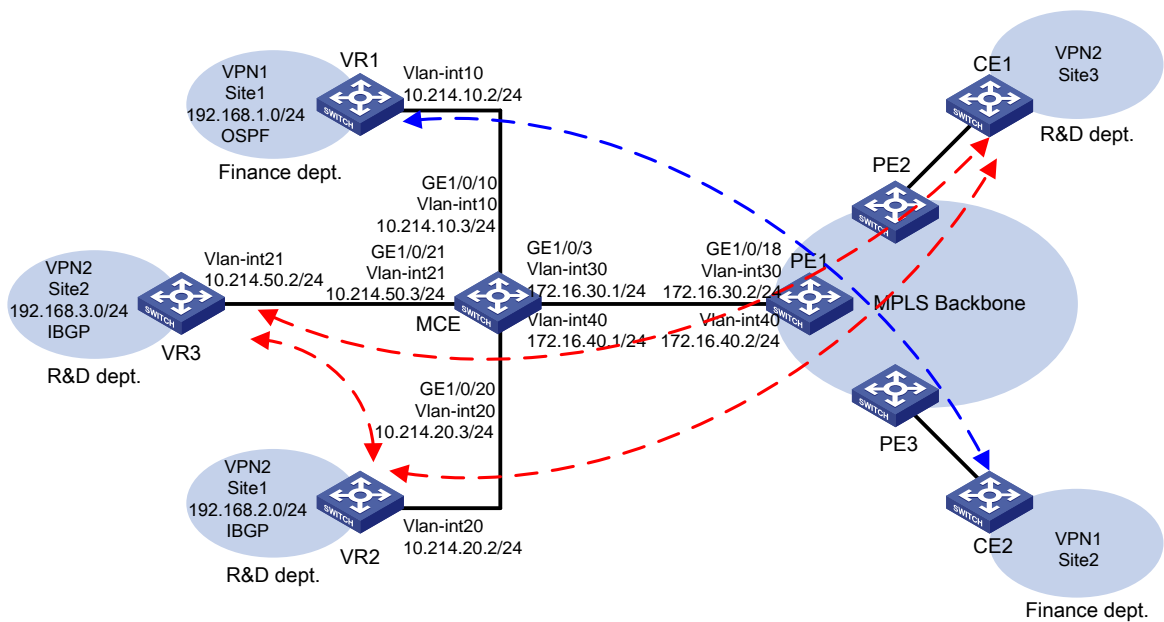
Network requirements

As shown in [Figure 114](#), 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.
- The MCE exchanges routes with PE1 through BGP.
- VPN sites can exchange VPN routes through PEs.

Figure 114 Network diagram



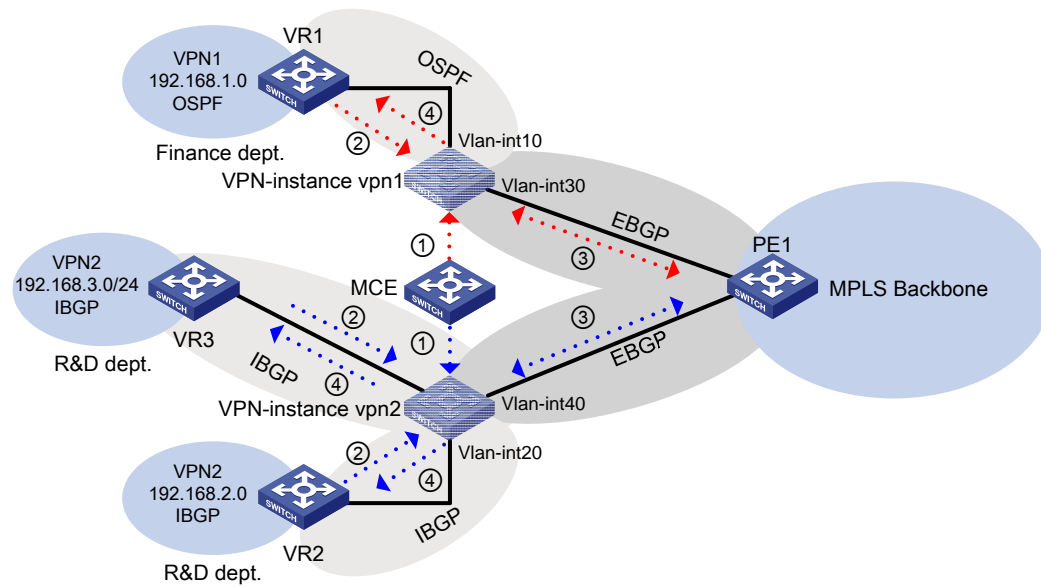
Requirements analysis

To isolate VPNs, 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 115 shows the order in which the MCE processes routing information for each VPN.

For the VPN sites to exchange VPN routes, 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, and redistribute the remote VPN routes to the local VPN sites.

IBGP requires a fully meshed network or a router reflector. In this example, configure the MCE as the IBGP route reflector.

Figure 115 Network diagram



Configuration restrictions and guidelines

The **ip binding vpn-instance** command removes the IP address of the bound interface. After you execute the **ip binding vpn-instance** command on an interface, you must re-configure an IP address for that interface.

Configuration procedures

This example only shows the configurations on the MCE and the connected devices VR1, VR2 and PE1.

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, add GigabitEthernet 1/0/10 to VLAN 10, and create VLAN-interface 10.

```
[MCE] vlan 10
[MCE-vlan10] port GigabitEthernet 1/0/10
[MCE-vlan10] quit
[MCE] interface Vlan-interface 10
```

Bind VLAN-interface 10 to VPN instance **vpn1**, and configure IP address 10.214.10.3/24 for the VLAN interface.

```
[MCE-Vlan-interface10] ip binding vpn-instance vpn1
[MCE-Vlan-interface10] ip address 10.214.10.3 24
```

Create VLAN 20, and add GigabitEthernet 1/0/20 to VLAN 20.

```
[MCE-Vlan-interface10] quit
[MCE] vlan 20
[MCE-vlan20] port GigabitEthernet 1/0/20
[MCE-vlan20] quit
```

Create VLAN-interface 20.

```
[MCE] interface Vlan-interface 20
```

Bind VLAN-interface 20 to VPN instance **vpn2**.

```
[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 add GigabitEthernet 1/0/21 to VLAN 21.

```
[MCE] vlan 21
[MCE-vlan21] port GigabitEthernet 1/0/21
[MCE-vlan21] quit
```

Create VLAN-interface 21, 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 GigabitEthernet 1/0/3 to the two VLANs.

```
[MCE] interface GigabitEthernet 1/0/3
[MCE-GigabitEthernet1/0/3] port link-type trunk
[MCE-GigabitEthernet1/0/3] port trunk permit vlan 30 40
[MCE-GigabitEthernet1/0/3] quit
```

Create VLAN-interface 30, and bind it to VPN instance **vpn1**.

```
[MCE] interface Vlan-interface 30
[MCE-Vlan-interface30] ip binding vpn-instance vpn1
```

Configure an IP address for the VLAN interface.

```
[MCE-Vlan-interface30] ip address 172.16.30.1 24
[MCE-Vlan-interface30] quit
```


Create VLAN-interface 40, and bind it to VPN instance **vpn2**.

```
[MCE] interface Vlan-interface 40
[MCE-Vlan-interface40] ip binding vpn-instance vpn2
```

Configure an IP address for the VLAN interface.

```
[MCE-Vlan-interface40] ip address 172.16.40.1 24
[MCE-Vlan-interface40] quit
```

On PE1, configure the VPN instances and RDs, and bind VPN instances to the interface that connects to the MCE. (Details not shown.)

HP recommends configuring 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 VR1, configure IP address 192.168.1.1/24 for the interface that connects to VPN 1 site 1, and configure VLAN settings. (Details not shown.)

On VR1, 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, and 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, enable OSPF process 1 for VPN instance **vpn1**.

```
[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
```

Routing Tables: vpn1

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 VR2, configure IP address 10.214.20.2 for the interface that connects to the MCE. On VR3, 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 VR2. Configure IP address 10.214.50.3 for the interface that connects to VR3. (Details not shown.)

On VR2, enable BGP in AS 100.

```
<VR2> system-view
[VR2] bgp 100
[VR2-bgp] router-id 2.2.2.2
```

Specify the MCE at 10.214.20.3 as a BGP peer.

```
[VR2-bgp] peer 10.214.20.3 as-number 100
```

Advertise networks 192.168.2.0 and 10.214.20.0.

```
[VR2-bgp] network 192.168.2.0 24
[VR2-bgp] network 10.214.20.0 24
```

On VR3, enable BGP in AS 100.

```
<VR3> system-view
[VR3] bgp 100
[VR3-bgp] router-id 3.3.3.3
```

Specify the MCE as a BGP peer.

```
[VR3-bgp] peer 10.214.50.3 as-number 100
```

Advertise networks.

```
[VR3-bgp] network 192.168.3.0 24
[VR3-bgp] network 10.214.50.0 24
[VR3-bgp] network 3.3.3.3 32
```

On MCE, enable BGP in AS 100.

```
[MCE] bgp 100
```

Create BGP-VPN instance **vpn2**.

```
[MCE-bgp] ipv4-family vpn-instance vpn2
```

Specify BGP peers 10.214.20.2 and 10.214.50.2.

```
[MCE-bgp-vpn2] peer 10.214.20.2 as-number 100
[MCE-bgp-vpn2] peer 10.214.50.2 as-number 100
```

Advertise networks 10.214.20.0/24 and 10.214.50.0/24.

```
[MCE-bgp-vpn2] network 10.214.20.0 24
[MCE-bgp-vpn2] network 10.214.50.0 24
```

Configure the MCE as a router reflector, and configure VR2 and VR3 as its clients.

```
[MCE-bgp-vpn2] peer 10.214.20.2 reflect-client
[MCE-bgp-vpn2] peer 10.214.50.2 reflect-client
[MCE-bgp-vpn2] quit
```

Display the BGP routing table on the MCE.

```
[MCE-bgp] display bgp routing-table
```

Total Number of Routes: 3

BGP Local router ID is 4.4.4.4

Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* i	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 GigabitEthernet 1/0/18 to VLAN 30 and VLAN 40.

```
<PE1> system-view
[PE1] interface GigabitEthernet 1/0/18
[PE1-GigabitEthernet1/0/18] port link-type trunk
[PE1-GigabitEthernet1/0/18] port trunk permit vlan 30 40
[PE1-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] ipv4-family vpn-instance vpn1
[PE1-bgp-vpn1] quit
[PE1-bgp] ipv4-family vpn-instance vpn2
[PE1-bgp-vpn2] quit
```

On the MCE, create BGP-VPN instance **vpn1**, and redistribute OSPF routes for **vpn1**.

```
[MCE-bgp] ipv4-family vpn-instance vpn1
[MCE-bgp-vpn1] import-route ospf
```

On the MCE, specify PE 1 as an EBGP peer in AS 200 and 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] network 172.16.30.0 24
```

```
[MCE-bgp-vpn1] quit
```

On PE 1, specify the MCE as an EBGP peer in AS 100 and advertise network 172.16.30.0 for BGP-VPN instance **vpn1**.

```
[PE1-bgp] ipv4-family vpn-instance vpn1
[PE1-bgp-vpn1] peer 172.16.30.1 as-number 100
[PE1-bgp-vpn1] network 172.16.30.0 24
[PE1-bgp-vpn1] quit
```

On the MCE, specify EBGP peer 172.16.40.2 in AS 200 and advertise network 172.16.40.0 for BGP-VPN instance **vpn2**.

```
[MCE-bgp] ipv4-family vpn-instance vpn2
[MCE-bgp-vpn2] peer 172.16.40.2 as-number 200
[MCE-bgp-vpn2] network 172.16.40.0 24
```

On PE 1, specify EBGP peer 172.16.40.1 in AS 100 and advertise network 172.16.40.0 for BGP-VPN instance **vpn2**.

```
[PE1-bgp] ipv4-family vpn-instance vpn2
[PE1-bgp-vpn2] peer 172.16.40.1 as-number 100
[PE1-bgp-vpn2] network 172.16.40.0 24
```

Verifying the configuration

On the MCE, display EBGP peers for VPN instance **vpn1**.

```
[MCE-bgp-vpn2] display bgp vpnv4 vpn-instance vpn1 peer
```

```
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 PE1.

On PE1, display the routing table for VPN instance **vpn1**.

```
[PE1-bgp-vpn2] display ip routing-table vpn-instance vpn1
Routing Tables: 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-bgp-vpn2] display bgp vpnv4 vpn-instance vpn2 peer
```

```
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 PE1.

On PE1, display the routing table for VPN instance **vpn2**.

```
[PE1-bgp-vpn2] display ip routing-table vpn-instance vpn2
```

```
Routing Tables: vpn1
```

```
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 GigabitEthernet1/0/3
port link-type trunk
port trunk permit vlan 1 30 40
#
interface GigabitEthernet1/0/10
port access vlan 10
#
interface GigabitEthernet1/0/20
port access vlan 20
#
interface GigabitEthernet1/0/21
port access vlan 21
#
bgp 100
undo synchronization
#
ipv4-family vpn-instance vpn1
peer 172.16.30.2 as-number 200
network 172.16.30.0 255.255.255.0
import-route ospf 1
#
ipv4-family vpn-instance vpn2
peer 10.214.20.2 as-number 100
peer 172.16.40.2 as-number 200
peer 10.214.50.2 as-number 100
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 reflect-client

```

```

    peer 10.214.50.2 reflect-client
#
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 GigabitEthernet1/0/18
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan 30 40
#
bgp 200
    undo synchronization
#
    ipv4-family vpn-instance vpn1
        peer 172.16.30.1 as-number 100
        network 172.16.30.0 255.255.255.0
#
    ipv4-family vpn-instance vpn2
        peer 172.16.40.1 as-number 100
        network 172.16.40.0 255.255.255.0

```

Mirroring configuration examples

This chapter provides mirroring configuration examples.

Table 7 Mirroring types and scenarios

Mirroring type	Application scenario
Port mirroring	All traffic to be monitored is forwarded to the switch that connects to the data monitoring device.
Layer 2 remote mirroring	The mirroring source and mirroring destination are located on different devices on the same Layer 2 network.
Layer 3 remote mirroring	The mirroring source and the mirroring destination are separated by IP networks.
Local traffic mirroring	The device that monitors the traffic is directly connected to the device that the traffic passes through.
Remote traffic mirroring	The device that monitors the traffic is <i>not</i> directly connected to the device that the traffic passes through.

Example: Configuring local port mirroring

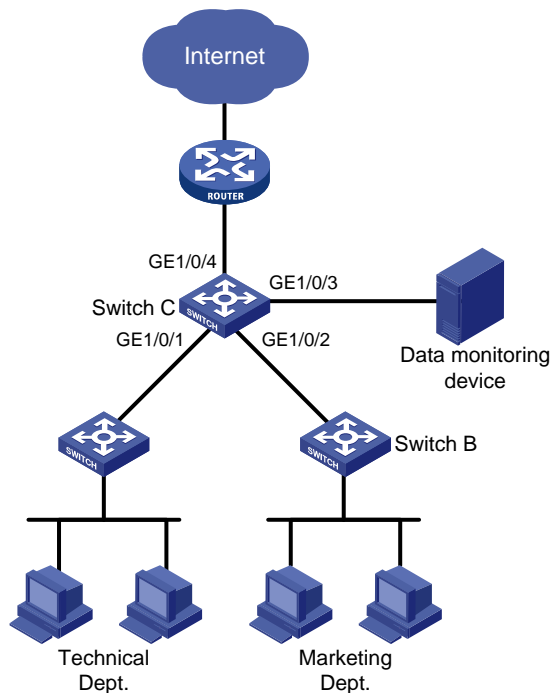
Applicable product matrix

Product series	Software version
HP 5500 EI	Release series 2220
HP 5500 SI	

Network requirements

As shown in [Figure 116](#), configure local port mirroring to monitor the Internet traffic and bidirectional traffic of the Marketing Department and the Technical Department.

Figure 116 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. The data monitoring device receives and analyzes only the mirrored traffic and not a mix of mirrored traffic and correctly forwarded traffic.

Configuration procedures

Create local mirroring group 1.

```
<SwitchC> system-view
[SwitchC] mirroring-group 1 local
```

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as the source ports of the mirroring group. Configure the mirroring group to monitor the incoming traffic of the ports.

```
[SwitchC] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2
inbound
```

Configure GigabitEthernet 1/0/3 as the monitor port of the mirroring group.

```
[SwitchC] mirroring-group 1 monitor-port GigabitEthernet 1/0/3
```

Disable the spanning tree feature on GigabitEthernet 1/0/3 to make sure mirroring operates correctly.

```
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] undo stp enable
[SwitchC-GigabitEthernet1/0/3] quit
```

Verifying the configuration

Display information about mirroring group 1 on Switch C.

```
[SwitchC] display mirroring-group 1
mirroring-group 1:
  type: local
  status: active
  mirroring port:
    GigabitEthernet1/0/1  inbound
    GigabitEthernet1/0/2  inbound
  monitor port: GigabitEthernet1/0/3
```

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
  mirroring-group 1 local
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/3
  port link-mode bridge
  stp disable
  mirroring-group 1 monitor-port
#
```

Example: Configuring Layer 2 remote port mirroring

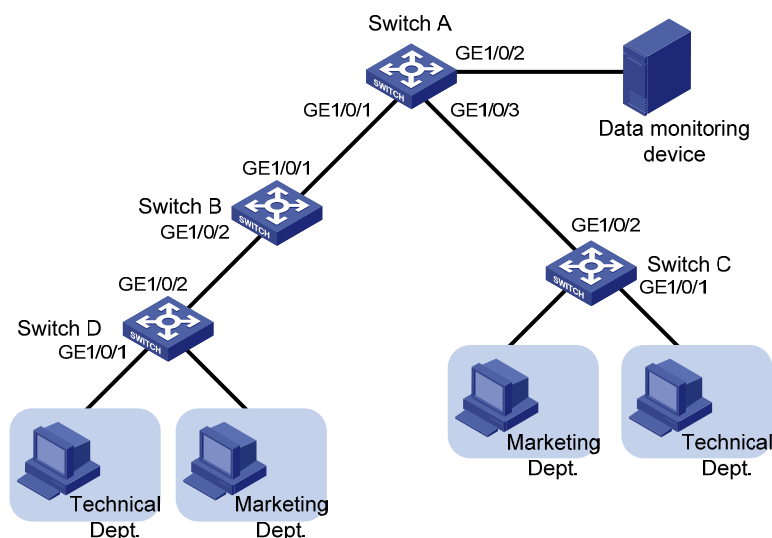
Applicable product matrix

Product series	Software version
HP 5500 EI	Release series 2220
HP 5500 SI	

Network requirements

As shown in [Figure 117](#), configure Layer 2 remote port mirroring to monitor the outgoing traffic of the Technical Departments.

Figure 117 Network diagram



Configuration restrictions and guidelines

When you configure the source device, follow these restrictions and guidelines:

- A remote source group contains only one egress port.
- You cannot configure a port of an existing mirroring group as an egress port.
- Only a static VLAN that already exists can be configured as a remote probe VLAN.
- Use a remote probe VLAN only for port mirroring.

- A remote probe VLAN belongs to only one remote source group.
- Specify an unused VLAN as the remote probe VLAN.

When you configure the destination device, follow these restrictions and guidelines:

- You cannot configure a port of an existing mirroring group as a destination port.
- Use a monitor port only for port mirroring.
- Only a static VLAN that already exists can be configured as a remote probe VLAN.
- Use a remote probe VLAN only for port mirroring.
- A remote probe VLAN belongs to only one remote destination group.
- Specify an unused VLAN as the remote probe VLAN.

Configuration procedures

Configuring Switch A (the destination device)

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 as trunk ports to permit the packets from VLAN 2 to pass through.

```
<SwitchA> system-view
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 2
[SwitchA-GigabitEthernet1/0/3] quit
```

Create a remote destination group.

```
[SwitchA] mirroring-group 1 remote-destination
```

Create VLAN 2, which is to be configured as the remote probe VLAN.

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

Configure VLAN 2 as the remote probe VLAN and GigabitEthernet 1/0/2 as the monitor port in the mirroring group.

```
[SwitchA] mirroring-group 1 remote-probe vlan 2
[SwitchA] mirroring-group 1 monitor-port GigabitEthernet 1/0/2
```

Assign the monitor port to VLAN 2. Because the mirrored packets do not need to be VLAN tagged, configure the monitor port as an access port.

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port access vlan 2
```

Disable the spanning tree feature on GigabitEthernet 1/0/2 to make sure mirroring operates correctly.

```
[SwitchC-GigabitEthernet1/0/2] undo stp enable
[SwitchA-GigabitEthernet1/0/2] quit
```

Configuring Switch B (the intermediate device)

```
# Create VLAN 2, which is to be configured as the remote probe VLAN.
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] quit

# Configure GigabitEthernet 1/0/1 as a trunk port to permit the packets from VLAN 2 to pass through.
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchB-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 as a trunk port to permit the packets from VLAN 2 to pass through.
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 2
[SwitchB-GigabitEthernet1/0/2] quit
```

Configuring Switch C and Switch D (the source device)

```
# Create a remote source group.
<SwitchC> system-view
[SwitchC] mirroring-group 1 remote-source

# Create VLAN 2, which is to be configured as the remote probe VLAN.
[SwitchC] vlan 2
[SwitchC-vlan2] quit

# Configure VLAN 2 as the remote probe VLAN.
[SwitchC] mirroring-group 1 remote-probe vlan 2

# Configure the mirroring group to monitor the incoming traffic of GigabitEthernet 1/0/1.
[SwitchC] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 inbound

# Configure GigabitEthernet 1/0/2 as the egress port.
[SwitchC] mirroring-group 1 monitor-egress GigabitEthernet 1/0/2

# Configure GigabitEthernet 1/0/2 as a trunk port to permit the packets from VLAN 2 to pass through.
[SwitchC] interface GigabitEthernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-type trunk
[SwitchC-GigabitEthernet1/0/2] port trunk permit vlan 2
[SwitchC-GigabitEthernet1/0/2] quit

# Disable the spanning tree and MAC address learning features on GigabitEthernet 1/0/2 to make sure mirroring operates correctly.
[SwitchC-GigabitEthernet1/0/2] undo stp enable
[SwitchC-GigabitEthernet1/0/2] mac-address mac-learning disable
[SwitchC-GigabitEthernet1/0/2] quit
```

NOTE:

Configure Switch D in the same way that Switch C is configured. Details are not shown here.

Verifying the configuration

Display information about mirroring group 1 on Switch C.

```
[SwitchC] display mirroring-group 1
mirroring-group 1:
  type: remote-source
  status: active
  mirroring port:
    GigabitEthernet1/0/1 inbound
  reflector port:
  monitor egress port: GigabitEthernet1/0/2
  remote-probe VLAN: 2
```

Display information about mirroring group 1 on Switch A.

```
[SwitchA] display mirroring-group 1
mirroring-group 1:
  type: remote-destination
  status: active
  monitor port: GigabitEthernet1/0/2
  remote-probe VLAN: 2
```

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```
#
  mirroring-group 1 remote-destination
  mirroring-group 1 remote-probe vlan 2
#
vlan 2
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 1 to 2
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 2
  stp disable
  mirroring-group 1 monitor-port
#
interface GigabitEthernet1/0/3
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 1 to 2
```

- Switch B:


```
#
vlan 2
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 1 to 2
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 1 to 2
#
```
- Switch C:


```
#
mirroring-group 1 remote-source
mirroring-group 1 remote-probe vlan 2
#
vlan 2
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  mirroring-group 1 mirroring-port
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 1 to 2
  stp disable
  mac-address mac-learning disable
  mirroring-group 1 monitor-egress
#
```

Example: Configuring Layer 3 remote port mirroring

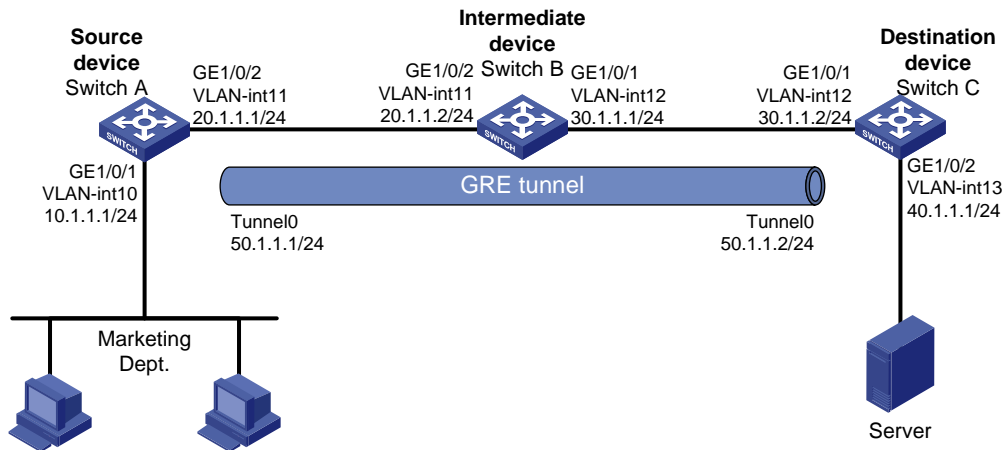
Applicable product matrix

Product series	Software version
HP 5500 EI	Release series 2220

Network requirements

As shown in [Figure 118](#), the network uses OSPF to advertise routes between the subnets. Configure Layer 3 remote port mirroring to monitor the bidirectional traffic of the Marketing Department.

Figure 118 Network diagram



Configuration restrictions and guidelines

When you configure a GRE over IPv4 tunnel to connect the company, the tunnel source and destination identify the tunnel. Make sure of the following:

- The configurations on the tunnel ends are the same.
- The source/destination address for an end is the destination/source for the remote end.

Configuration procedures

Configuring Switch A (the source device)

Create VLAN-interface 10 and VLAN-interface 11.

```
<SwitchA> system-view
[SwitchA] vlan 10 to 11
Please wait... Done.
[SwitchA] interface Vlan-interface 10
[SwitchA-Vlan-interface10] ip address 10.1.1.1 24
[SwitchA-Vlan-interface10] quit
[SwitchA] interface Vlan-interface 11
[SwitchA-Vlan-interface11] ip address 20.1.1.1 24
[SwitchA-Vlan-interface11] quit
```

Assign GigabitEthernet 1/0/1 to VLAN 10 and GigabitEthernet 1/0/2 to VLAN 11.

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



```

[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 11
[SwitchA-GigabitEthernet1/0/2] quit

# Create tunnel interface Tunnel 0, and configure its IP address and mask.
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ip address 50.1.1.1 24

# Configure Tunnel 0 to operate in GRE over IPv4 tunnel mode, and configure the source and destination
IP addresses for it.
[SwitchA-Tunnel0] tunnel-protocol gre
[SwitchA-Tunnel0] source 20.1.1.1
[SwitchA-Tunnel0] destination 30.1.1.2
[SwitchA-Tunnel0] quit

# Configure service loopback group 1 and specify its service type as tunnel.
[SwitchA] service-loopback group 1 type tunnel

# Assign an unused port (GigabitEthernet 1/0/3 in this example) to service loopback group 1.
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] undo stp enable
[SwitchA-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-GigabitEthernet1/0/3] quit

# Reference service loopback group 1 on the tunnel interface.
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] service-loopback-group 1
[SwitchA-Tunnel0] quit

# Enable the OSPF protocol to advertise routes to the subnets where the VLAN interfaces and the tunnel
interface reside.
[SwitchA] ospf 1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 50.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit

# Create local mirroring group 1.
[SwitchA] mirroring-group 1 local

# Configure GigabitEthernet 1/0/1 as a source port and Tunnel 0 as the monitor port of local mirroring
group 1.
[SwitchA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both
[SwitchA] mirroring-group 1 monitor-port tunnel 0

```

Configuring Switch B (the intermediate device)

```

# Create VLAN-interface 11 and VLAN-interface 12.
<SwitchB> system-view

```

```
[SwitchB] vlan 11 to 12
Please wait... Done.
[SwitchB] interface Vlan-interface 11
[SwitchB-Vlan-interfacel1] ip address 20.1.1.2 24
[SwitchB-Vlan-interfacel1] quit
[SwitchB] interface Vlan-interface 12
[SwitchB-Vlan-interfacel2] ip address 30.1.1.1 24
[SwitchB-Vlan-interfacel2] quit
```

Assign GigabitEthernet 1/0/2 to VLAN 11 and GigabitEthernet 1/0/1 to VLAN 12.

```
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 11
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 12
[SwitchB-GigabitEthernet1/0/1] quit
```

Enable the OSPF protocol to advertise routes to the subnets where VLAN-interface 11 and VLAN-interface 12 reside.

```
[SwitchB] ospf 1
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configuring Switch C (the destination device)

Create VLAN-interface 12 and VLAN-interface 13.

```
<SwitchC> system-view
[SwitchC] vlan 12 to 13
Please wait... Done.
[SwitchC] interface Vlan-interface 12
[SwitchC-Vlan-interfacel2] ip address 30.1.1.2 24
[SwitchC-Vlan-interfacel2] quit
[SwitchC] interface Vlan-interface 13
[SwitchC-Vlan-interfacel3] ip address 40.1.1.1 24
```

Assign GigabitEthernet 1/0/1 to VLAN 12 and GigabitEthernet 1/0/2 to VLAN 13.

```
[SwitchC-Vlan-interfacel3] quit
[SwitchC] interface GigabitEthernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 12
[SwitchC-GigabitEthernet1/0/1] quit
[SwitchC] interface GigabitEthernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port access vlan 13
[SwitchC-GigabitEthernet1/0/2] quit
```

Create tunnel interface Tunnel 0, and configure its IP address and mask.

```

[SwitchC] interface tunnel 0
[SwitchC-Tunnel0] ip address 50.1.1.2 24

# Configure Tunnel 0 to operate in GRE over IPv4 tunnel mode, and configure the source and destination
IP addresses for it.
[SwitchC-Tunnel0] tunnel-protocol gre
[SwitchC-Tunnel0] source 30.1.1.2
[SwitchC-Tunnel0] destination 20.1.1.1
[SwitchC-Tunnel0] quit

# Configure service loopback group 1 and specify its service type as tunnel.
[SwitchC] service-loopback group 1 type tunnel

# Assign an unused port (GigabitEthernet 1/0/3 in this example) to service loopback group 1.
[SwitchC] interface GigabitEthernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] undo stp enable
[SwitchC-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchC-GigabitEthernet1/0/3] quit

# Reference service loopback group 1 on the tunnel interface.
[SwitchC] interface tunnel 0
[SwitchC-Tunnel0] service-loopback-group 1
[SwitchC-Tunnel0] quit

# Enable the OSPF protocol to advertise routes to the subnets where the VLAN interfaces and the tunnel
interface reside.
[SwitchC] ospf 1
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 50.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit

# Create local mirroring group 1.
[SwitchA] mirroring-group 1 local

# Configure the mirroring group to monitor the incoming traffic of the source port GigabitEthernet
1/0/1.
[SwitchC] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 inbound
# Configure GigabitEthernet 1/0/2 as the monitor port of local mirroring group 1.
[SwitchC] mirroring-group 1 monitor-port gigabitethernet 1/0/2

```

Verifying the configuration

```

# Display information about mirroring group 1 on Switch A.
[SwitchA] display mirroring-group 1
mirroring-group 1:
    type: local
    status: active

```

```

mirroring port:
    GigabitEthernet1/0/1  both
monitor port: Tunnel0

# Display information about mirroring group 1 on Switch C.
[SwitchC] display mirroring-group 1
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet1/0/1  inbound
    monitor port: GigabitEthernet1/0/2

```

Configuration files

- Switch A:

```

#
 mirroring-group 1 local
#
 service-loopback group 1 type tunnel
#
vlan 10 to 11
#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface11
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
 mirroring-group 1 mirroring-port both
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 stp disable
 port service-loopback group 1
#
interface Tunnel0
 ip address 50.1.1.1 255.255.255.0
 source 20.1.1.1
 destination 30.1.1.2

```

```

service-loopback-group 1
mirroring-group 1 monitor-port
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 20.1.1.0 0.0.0.255
network 50.1.1.0 0.0.0.255

```

- Switch B:

```

#
vlan 11 to 12
#
interface Vlan-interface11
ip address 20.1.1.2 255.255.255.0
#
interface Vlan-interface12
ip address 30.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 12
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 11
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 20.1.1.0 0.0.0.255

```

- Switch C:

```

#
mirroring-group 1 local
#
service-loopback group 1 type tunnel
#
vlan 12 to 13
#
interface Vlan-interface12
ip address 30.1.1.2 255.255.255.0
#
interface Vlan-interface13
ip address 40.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode bridge

```

```

port link-type trunk
port trunk permit vlan 1 12
mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 13
mirroring-group 1 monitor-port
#
interface GigabitEthernet1/0/3
port link-mode bridge
stp disable
port service-loopback group 1
#
interface Tunnel0
ip address 50.1.1.1 255.255.255.0
source 30.1.1.2
destination 20.1.1.1
service-loopback-group 1
#
ospf 1
area 0.0.0.0
network 30.1.1.0 0.0.0.255
network 40.1.1.0 0.0.0.255
network 50.1.1.0 0.0.0.255

```

Example: Configuring local traffic mirroring

Applicable product matrix

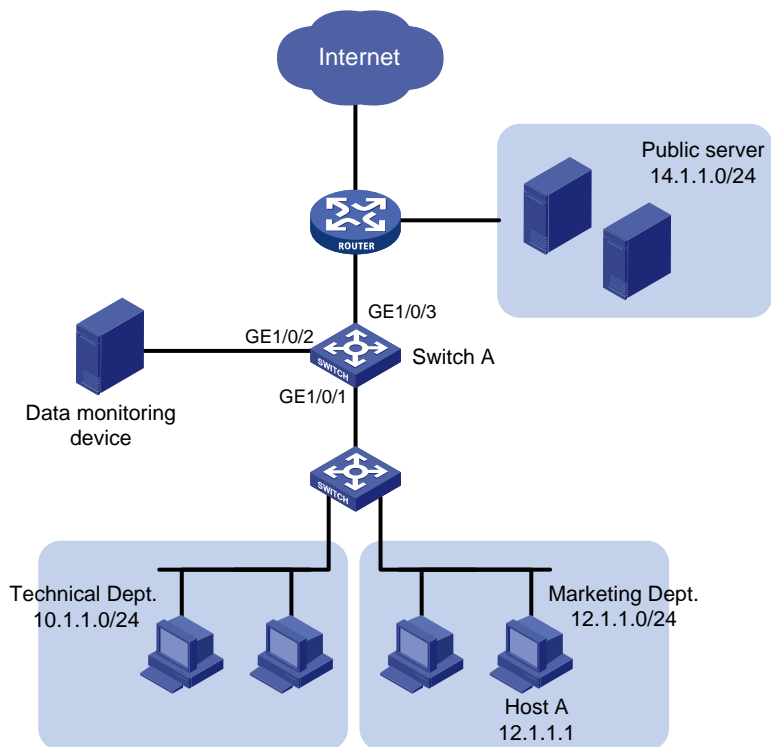
Product series	Software version
HP 5500 EI	Release series 2220
HP 5500 SI	

Network requirements

As shown in [Figure 119](#), configure local traffic mirroring to mirror the following traffic:

- HTTP traffic sent by the Technical Department to access the Internet.
- Packets that Host A in the Marketing Department receives from the public server cluster during non-working hours from 18:00 to 08:30 (the next day) on working days.

Figure 119 Network diagram



Configuration procedures

1. Configure a QoS policy that mirrors Internet traffic from the Technical Department:

Create ACL 3000 and configure a rule to permit packets from the Technical Department to access the Internet.

```
<SwitchA> system-view
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule permit tcp destination-port eq 80 source 10.1.1.0
0.0.0.255
[SwitchA-acl-adv-3000] quit
```

Create traffic class **classifier_research**, and then configure the match criterion as ACL 3000.

```
[SwitchA] traffic classifier classifier_research
[SwitchA-classifier-classifier_research] if-match acl 3000
[SwitchA-classifier-classifier_research] quit
```

Create traffic behavior **behavior_research**, and then configure the action of mirroring traffic to GigabitEthernet 1/0/2.

```
[SwitchA] traffic behavior behavior_research
[SwitchA-behavior-behavior_research] mirror-to interface GigabitEthernet 1/0/2
[SwitchA-behavior-behavior_research] quit
```

Create QoS policy **policy_research**, and then associate traffic class **classifier_research** with traffic behavior **behavior_research** in the QoS policy.

```
[SwitchA] qos policy policy_research
```

```
[SwitchA-qospolicy-policy_research] classifier classifier_research behavior
behavior_research
```

```
[SwitchA-qospolicy-policy_research] quit
```

2. Configure a QoS policy that mirrors traffic received by Host A from the public server:

Configure two time ranges named **off-work1** and **off-work2** to cover the time from 0:00 to 8:30 and 18:00 to 24:00 on working days, respectively.

```
[SwitchA] time-range off-work1 0:00 to 8:30 working-day
```

```
[SwitchA] time-range off-work2 18:00 to 24:00 working-day
```

Create ACL 3001, and configure two rules to permit packets from the public server to Host A in non-working hours on working days.

```
[SwitchA] acl number 3001
```

```
[SwitchA-acl-adv-3001] rule permit ip destination 12.1.1.1 0.0.0.0 source 14.1.1.0
0.0.0.255 time-range off-work1
```

```
[SwitchA-acl-adv-3001] rule permit ip destination 12.1.1.1 0.0.0.0 source 14.1.1.0
0.0.0.255 time-range off-work2
```

```
[SwitchA-acl-adv-3001] quit
```

Create traffic class **classifier_market**, and then configure the match criterion as ACL 3001.

```
[SwitchA] traffic classifier classifier_market
```

```
[SwitchA-classifier-classifier_market] if-match acl 3001
```

```
[SwitchA-classifier-classifier_market] quit
```

Create traffic behavior **behavior_market**, and then configure the action of mirroring traffic to GigabitEthernet 1/0/2.

```
[SwitchA] traffic behavior behavior_market
```

```
[SwitchA-behavior-behavior_market] mirror-to interface GigabitEthernet 1/0/2
```

```
[SwitchA-behavior-behavior_market] quit
```

Create QoS policy **policy_market**, and then associate traffic class **classifier_market** with traffic behavior **behavior_market** in the QoS policy.

```
[SwitchA] qos policy policy_market
```

```
[SwitchA-qospolicy-policy_market] classifier classifier_market behavior
behavior_market
```

```
[SwitchA-qospolicy-policy_market] quit
```

3. Apply the QoS policies:

Apply QoS policy **policy_research** to the incoming packets of GigabitEthernet 1/0/1.

```
[SwitchA] interface GigabitEthernet 1/0/1
```

```
[SwitchA-GigabitEthernet1/0/1] qos apply policy policy_research inbound
```

Apply QoS policy **policy_market** to the outgoing packets of GigabitEthernet 1/0/1.

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

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

Verifying the configuration

Display local traffic mirroring information on Switch A.

```
[SwitchA] display qos policy interface GigabitEthernet 1/0/1
```



```

Interface: GigabitEthernet1/0/1

Direction: Inbound

Policy: policy_research
Classifier: classifier_research
Operator: AND
Rule(s) : If-match acl 3000
Behavior: behavior_research
Mirror enable:
Mirror type: interface
Mirror destination: GigabitEthernet1/0/2

Direction: Outbound

Policy: policy_market
Classifier: classifier_market
Operator: AND
Rule(s) : If-match acl 3001
Behavior: behavior_market
Mirror enable:
Mirror type: interface
Mirror destination: GigabitEthernet1/0/2

```

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```

#
time-range off-work1 00:00 to 08:30 working-day
time-range off-work2 18:00 to 24:00 working-day
#
acl number 3000
rule 0 permit tcp source 10.1.1.0 0.0.0.255 destination-port eq www
acl number 3001
rule 0 permit ip source 14.1.1.0 0.0.0.255 destination 12.1.1.1 0 time-range off-work1
rule 5 permit ip source 14.1.1.0 0.0.0.255 destination 12.1.1.1 0 time-range off-work2
#
traffic classifier classifier_research operator and
if-match acl 3000
traffic classifier classifier_market operator and
if-match acl 3001
#
traffic behavior behavior_research
mirror-to interface GigabitEthernet1/0/2
traffic behavior behavior_market
mirror-to interface GigabitEthernet1/0/2
#

```

```
qos policy policy_research
  classifier classifier_research behavior behavior_research
qos policy policy_market
  classifier classifier_market behavior behavior_market
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  qos apply policy policy_research inbound
  qos apply policy policy_market outbound
#
```

Example: Configuring remote traffic mirroring

Applicable product matrix

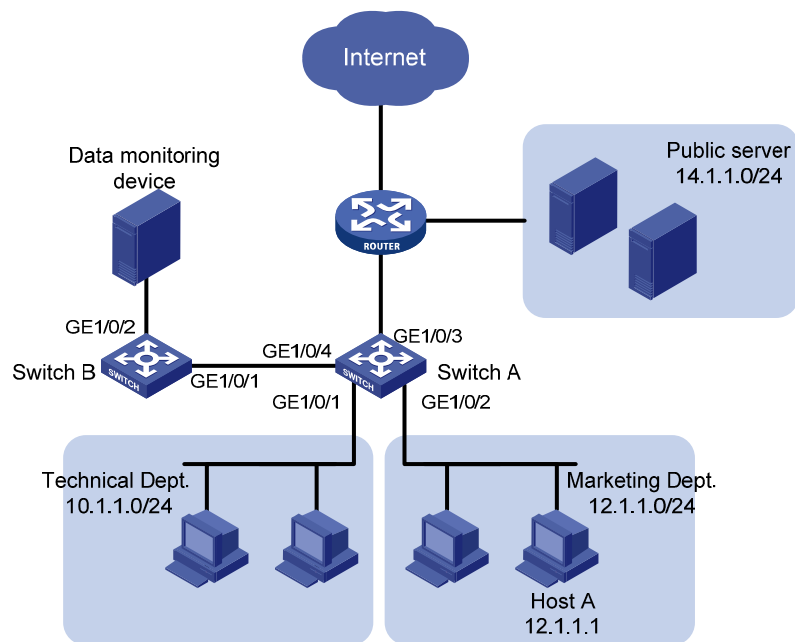
Product series	Software version
HP 5500 EI	Release series 2220
HP 5500 SI	

Network requirements

As shown in [Figure 120](#), configure remote traffic mirroring to mirror the following traffic:

- HTTP traffic sent by the Technical Department to access the Internet.
- Packets that Host A in the Marketing Department receives from the public server cluster during the non-working hours from 18:00 to 8:30 (the next day) on working days.

Figure 120 Network diagram



Configuration restrictions and guidelines

Remote traffic mirroring is implemented by local traffic mirroring and Layer 2 remote port mirroring. For the related configuration restrictions and guidelines, see "[Configuration restrictions and guidelines.](#)"

Configuration procedures

Configuring Switch A

Create ACL 3000, and configure a rule to permit packets from the Technical Department to access the Internet.

```
<SwitchA> system-view
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule permit tcp destination-port eq 80 source 10.1.1.0 0.0.0.255
[SwitchA-acl-adv-3000] quit
```

Create traffic class **classifier_research**, and then configure the match criterion as ACL 3000.

```
[SwitchA] traffic classifier classifier_research
[SwitchA-classifier-classifier_research] if-match acl 3000
[SwitchA-classifier-classifier_research] quit
```

Create traffic behavior **behavior_research**, and then configure the action of mirroring traffic to GigabitEthernet 1/0/4.

```
[SwitchA] traffic behavior behavior_research
[SwitchA-behavior-behavior_research] mirror-to interface GigabitEthernet 1/0/4
[SwitchA-behavior-behavior_research] quit
```

Create QoS policy **policy_research**, and then associate traffic class **classifier_research** with traffic behavior **behavior_research** in the QoS policy.

```
[SwitchA] qos policy policy_research
[SwitchA-qospolicy-policy_research] classifier classifier_research behavior
behavior_research
[SwitchA-qospolicy-policy_research] quit
```

Configure two time ranges named **off-work1** and **off-work2** to cover the time from 0:00 to 8:30 and 18:00 to 24:00 on working days, respectively.

```
[SwitchA] time-range off-work1 0:00 to 8:30 working-day
[SwitchA] time-range off-work2 18:00 to 24:00 working-day
```

Create ACL 3001, and configure two rules to permit packets from the public server to Host A in non-working hours on working days.

```
[SwitchA] acl number 3001
[SwitchA-acl-adv-3001] rule permit ip destination 12.1.1.1 0.0.0.0 source 14.1.1.0
0.0.0.255 time-range off-work1
[SwitchA-acl-adv-3001] rule permit ip destination 12.1.1.1 0.0.0.0 source 14.1.1.0
0.0.0.255 time-range off-work2
[SwitchA-acl-adv-3001] quit
```

Create traffic class **classifier_market**, and then configure the match criterion as ACL 3001.

```
[SwitchA] traffic classifier classifier_market
[SwitchA-classifier-classifier_market] if-match acl 3001
[SwitchA-classifier-classifier_market] quit
```

Create traffic behavior **behavior_market**, and then configure the action of mirroring traffic to GigabitEthernet 1/0/4.

```
[SwitchA] traffic behavior behavior_market
[SwitchA-behavior-behavior_market] mirror-to interface GigabitEthernet 1/0/4
[SwitchA-behavior-behavior_market] quit
```

Create QoS policy **policy_market**, and then associate traffic class **classifier_market** with traffic behavior **behavior_market** in the QoS policy.

```
[SwitchA] qos policy policy_market
[SwitchA-qospolicy-policy_market] classifier classifier_market behavior behavior_market
[SwitchA-qospolicy-policy_market] quit
```

Apply QoS policy **policy_research** to the incoming packets of GigabitEthernet 1/0/1.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos apply policy policy_research inbound
[SwitchA-GigabitEthernet1/0/1] quit
```

Apply QoS policy **policy_market** to the outgoing packets of GigabitEthernet 1/0/2.

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] qos apply policy policy_market outbound
[SwitchA-GigabitEthernet1/0/2] quit
```

Create remote source group 1.

```
[SwitchA] mirroring-group 1 remote-source
```

Configure an unused VLAN (VLAN 2 in this example) as the remote probe VLAN.

```
[SwitchA] vlan 2
[SwitchA-vlan2] quit
[SwitchA] mirroring-group 1 remote-probe vlan 2

# Configure an unused port (GigabitEthernet 1/0/10 in this example) as a source port and
GigabitEthernet 1/0/4 as the egress port of remote source group 1.

[SwitchA] mirroring-group 1 mirroring-port GigabitEthernet 1/0/10 inbound
[SwitchA] mirroring-group 1 monitor-egress GigabitEthernet 1/0/4
```

NOTE:

Configure an unused port as a source port to prevent packets that pass through the port from being mirrored to the destination device through the remote mirroring group.

```
# Configure GigabitEthernet 1/0/4 as a trunk port to permit the packets from VLAN 2 to pass through.

[SwitchA] interface GigabitEthernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-type trunk
[SwitchA-GigabitEthernet1/0/4] port trunk permit vlan 2
[SwitchA-GigabitEthernet1/0/4] quit
```

Configuring Switch B

```
# Configure GigabitEthernet 1/0/1 as a trunk port to permit the packets from VLAN 2 to pass through.
<SwitchB> system-view
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchB-GigabitEthernet1/0/1] quit

# Create remote destination group 1.
[SwitchB] mirroring-group 1 remote-destination

# Configure VLAN 2 as the remote probe VLAN.
[SwitchB] vlan 2
[SwitchB-vlan2] quit
[SwitchB] mirroring-group 1 remote-probe vlan 2

# Configure GigabitEthernet 1/0/2 as the monitor port of the remote destination group.
[SwitchB] mirroring-group 1 monitor-port GigabitEthernet 1/0/2

# Assign the monitor port to VLAN 2. Because the mirrored packets do not need to be VLAN tagged,
configure the monitor port as an access port.
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port access vlan 2
[SwitchB-GigabitEthernet1/0/2] quit
```

Verifying the configuration

```
# Display remote traffic mirroring information on Switch A.
[SwitchA] display qos policy interface
```

```
Interface: GigabitEthernet1/0/1

Direction: Inbound

Policy: policy_research
Classifier: classifier_research
Operator: AND
Rule(s) : If-match acl 3000
Behavior: behavior_research
Mirror enable:
Mirror type: interface
Mirror destination: GigabitEthernet1/0/4
```

```
Interface: GigabitEthernet1/0/2

Direction: Outbound

Policy: policy_market
Classifier: classifier_market
Operator: AND
Rule(s) : If-match acl 3001
Behavior: behavior_market
Mirror enable:
Mirror type: interface
Mirror destination: GigabitEthernet1/0/4
```

Display information about mirroring group 1 on Switch A.

```
[SwitchA] display mirroring-group 1
mirroring-group 1:
  type: remote-source
  status: active
  mirroring port:
    GigabitEthernet1/0/10 inbound
  reflector port:
  monitor egress port: GigabitEthernet1/0/4
  remote-probe VLAN: 2
```

Display information about mirroring group 1 on Switch B.

```
[SwitchB] display mirroring-group 1
mirroring-group 1:
  type: remote-destination
  status: active
  monitor port: GigabitEthernet1/0/2
  remote-probe VLAN: 2
```

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```
#
mirroring-group 1 remote-source
mirroring-group 1 remote-probe vlan 2
#
time-range off-work1 00:00 to 08:30 working-day
time-range off-work2 18:00 to 24:00 working-day
#
acl number 3000
rule 0 permit tcp source 10.1.1.0 0.0.0.255 destination-port eq www
acl number 3001
rule 0 permit ip source 14.1.1.0 0.0.0.255 destination 12.1.1.1 0 time-range
off-work1
rule 5 permit ip source 14.1.1.0 0.0.0.255 destination 12.1.1.1 0 time-range
off-work2
#
vlan 2
#
traffic classifier classifier_research operator and
if-match acl 3000
traffic classifier classifier_market operator and
if-match acl 3001
#
traffic behavior behavior_research
mirror-to interface GigabitEthernet1/0/4
traffic behavior behavior_market
mirror-to interface GigabitEthernet1/0/4
#
qos policy policy_market
classifier classifier_market behavior behavior_market
qos policy policy_research
classifier classifier_research behavior behavior_research
#
interface GigabitEthernet1/0/1
port link-mode bridge
qos apply policy policy_research inbound
#
interface GigabitEthernet1/0/2
port link-mode bridge
qos apply policy policy_market outbound
#
interface GigabitEthernet1/0/4
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 2
mirroring-group 1 monitor-egress
#
interface GigabitEthernet1/0/10
```

```
port link-mode bridge
mirroring-group 1 mirroring-port inbound
```

- Switch B:

```
#
mirroring-group 1 remote-destination
mirroring-group 1 remote-probe vlan 2
#
vlan 2
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 2
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 2
mirroring-group 1 monitor-port
```

Example: Configuring traffic mirroring in a flexible way

Applicable product matrix

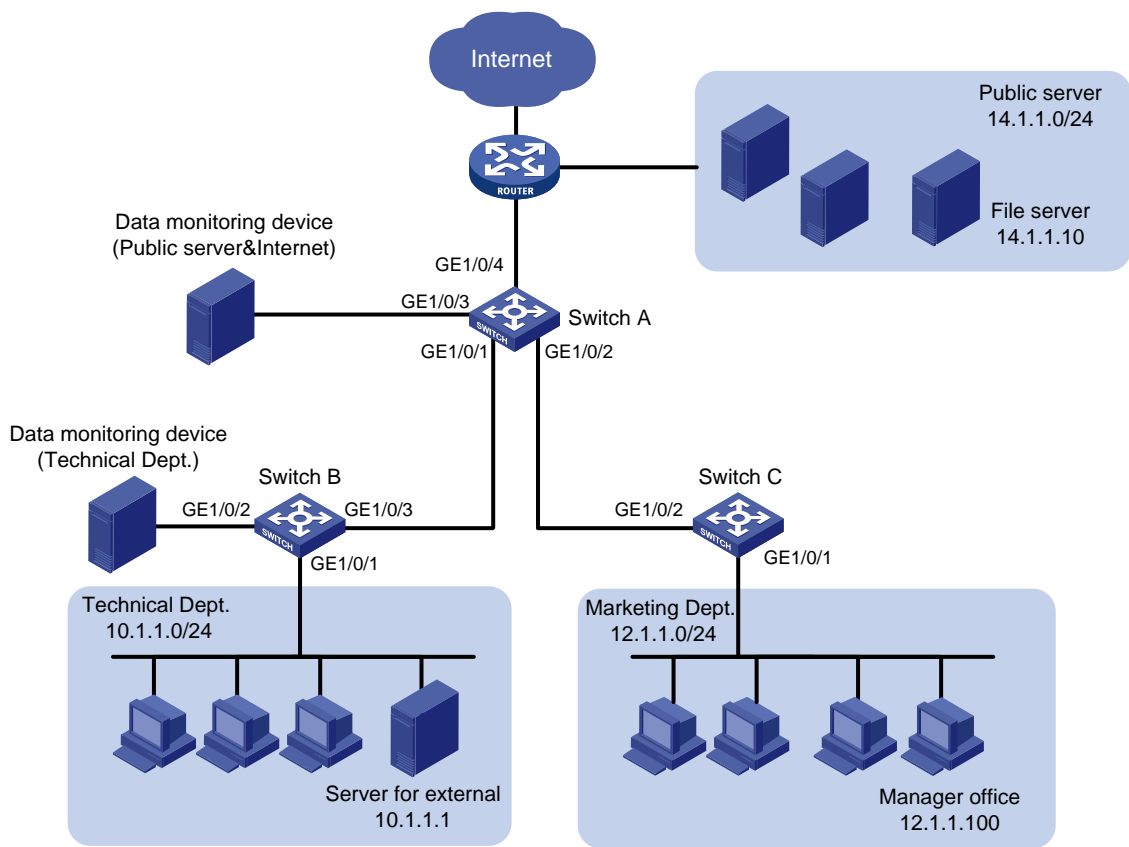
Product series	Software version
HP 5500 EI	Release series 2220
HP 5500 SI	

Network requirements

As shown in [Figure 121](#), configure traffic mirroring to monitor the network traffic by using the data monitoring devices as follows:

- Monitor the traffic from public servers. Monitor the traffic from the file server only in the non-working hours (18:00 to 8:30 of the next day) on working days.
- Monitor the traffic from the Marketing Department to the Internet, but do not monitor the traffic from the Marketing Department manager office to the Internet.
- Monitor the traffic from the Technical Department only in non-working hours (18:00 to 8:30 of the next day) on working days.

Figure 121 Network diagram



Requirements analysis

To filter data from a specific source, use one of the following methods:

- Apply a QoS policy of denying traffic to the outgoing interface of the mirrored data. The data from the specified source is not received by the data monitoring device.
- Configure a class-behavior association to permit the data from the specified source, and then issue the class-behavior association before the class-behavior association for mirroring. Data from the specified source is not mirrored.
- Use the **packet-filter** command on the outgoing interface of the mirrored data. The data from the specified source is not received by the data monitoring device.

Configuration procedures

Configuring Switch A to mirror traffic from the public servers

1. Configure a QoS policy to mirror traffic from all public servers:
Create ACL 2000 to permit packets from subnet 14.1.1.0/24.
<SwitchA> system-view

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 14.1.1.0 0.0.0.255
[SwitchA-acl-basic-2000] quit
```

Create traffic class **classifier_servers**, and then configure the match criterion as ACL 2000.

```
[SwitchA] traffic classifier classifier_servers
[SwitchA-classifier-classifier_servers] if-match acl 2000
[SwitchA-classifier-classifier_servers] quit
```

Create traffic behavior **behavior_servers**, and then configure the action of mirroring traffic to GigabitEthernet 1/0/3.

```
[SwitchA] traffic behavior behavior_servers
[SwitchA-behavior-behavior_servers] mirror-to interface GigabitEthernet 1/0/3
[SwitchA-behavior-behavior_servers] quit
```

Create QoS policy **policy_servers**, and then associate traffic class **classifier_servers** with traffic behavior **behavior_servers** in the QoS policy.

```
[SwitchA] qos policy policy_servers
[SwitchA-qospolicy-policy_servers] classifier classifier_servers behavior
behavior_servers
[SwitchA-qospolicy-policy_servers] quit
```

Apply QoS policy **policy_servers** to the incoming packets of GigabitEthernet 1/0/4.

```
[SwitchA] interface GigabitEthernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] qos apply policy policy_servers inbound
[SwitchA-GigabitEthernet1/0/4] quit
```

2. Configure a QoS policy to filter packets from the file server in working hours:

Create a working hour range named **work-time**, in which the working hour is from 8:30 to 18:00 on working days.

```
[SwitchA] time-range work-time 8:30 to 18:00 working-day
```

Create ACL 2001, and configure a rule to permit packets from 14.1.1.10 in working hours on working days.

```
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 14.1.1.10 0.0.0.0 time-range work-time
[SwitchA-acl-basic-2001] quit
```

Create traffic class **classifier_fileserver**, and then configure the match criterion as ACL 2001.

```
[SwitchA] traffic classifier classifier_fileserver
[SwitchA-classifier-classifier_fileserver] if-match acl 2001
[SwitchA-classifier-classifier_fileserver] quit
```

Create traffic behavior **behavior_fileserver**, and then configure the action of denying traffic.

```
[SwitchA] traffic behavior behavior_fileserver
[SwitchA-behavior-behavior_fileserver] filter deny
[SwitchA-behavior-behavior_fileserver] quit
```

Create QoS policy **policy_fileserver**, and then associate traffic class **classifier_fileserver** with traffic behavior **behavior_fileserver** in the QoS policy.

```
[SwitchA] qos policy policy_fileserver
[SwitchA-qospolicy-policy_fileserver] classifier classifier_fileserver behavior
behavior_fileserver
```

```
[SwitchA-qospolicy-policy_fileserver] quit
# Apply QoS policy policy_fileserver to the outgoing packets of GigabitEthernet 1/0/3.
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] qos apply policy policy_servers outbound
[SwitchA-GigabitEthernet1/0/3] quit
```

Configuring Switch A to mirror traffic from the Marketing Department to access the Internet

1. Create a traffic class and a traffic behavior for the packets:

Create ACL 3000, and configure a rule to permit packets from subnet 12.1.1.0/24.

```
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule permit tcp destination-port eq 80 source 12.1.1.0
0.0.0.255
[SwitchA-acl-adv-3000] quit
```

Create traffic class **classifier_market**, and then configure the match criterion as ACL 3000.

```
[SwitchA] traffic classifier classifier_market
[SwitchA-classifier-classifier_market] if-match acl 3000
[SwitchA-classifier-classifier_market] quit
```

Create traffic behavior **behavior_market**, and then configure the action of mirroring traffic to GigabitEthernet 1/0/3.

```
[SwitchA] traffic behavior behavior_market
[SwitchA-behavior-behavior_market] mirror-to interface GigabitEthernet 1/0/3
[SwitchA-behavior-behavior_market] quit
```

2. Create a traffic class and a traffic behavior for the packets from the manager office:

Create ACL 3001, and configure a rule to permit packets from 12.1.1.100.

```
[SwitchA] acl number 3001
[SwitchA-acl-adv-3001] rule permit tcp destination-port eq 80 source 12.1.1.100
0.0.0.0
[SwitchA-acl-adv-3001] quit
```

Create traffic class **classifier_market_mgr**, and then configure the match criterion as ACL 3001.

```
[SwitchA] traffic classifier classifier_market_mgr
[SwitchA-classifier-classifier_market_mgr] if-match acl 3001
[SwitchA-classifier-classifier_market_mgr] quit
```

Create traffic behavior **behavior_market_mgr**, and then configure the action of permitting traffic to pass through.

```
[SwitchA] traffic behavior behavior_market_mgr
[SwitchA-behavior-behavior_market_mgr] filter permit
[SwitchA-behavior-behavior_market_mgr] quit
```

3. Create a QoS policy to associate the traffic classes and traffic behaviors:

Create QoS policy **policy_market**.

```
[SwitchA] qos policy policy_market
```

Associate traffic class **classifier_market_mgr** with traffic behavior **behavior_market_mgr** in the QoS policy.

```
[SwitchA-qospolicy-policy_market] classifier classifier_market_mgr behavior
behavior_market_mgr
```

Associate traffic class **classifier_market** with traffic behavior **behavior_market** in the QoS policy.

```
[SwitchA-qospolicy-policy_market] classifier classifier_market behavior
behavior_market
```

Display the sequence of issuing the traffic classes and traffic behaviors.

```
[SwitchA-qospolicy-policy_market] display this
#
qos policy policy_market
 classifier classifier_market_mgr behavior behavior_market_mgr
 classifier classifier_market behavior behavior_market
#
return
[SwitchA-qospolicy-policy_market] quit
```

The output shows that the traffic class and traffic behavior for the manager office are issued first. The packets from the manager office to access the Internet are not mirrored.

4. Apply QoS policy **policy_market** to the incoming packets of GigabitEthernet 1/0/2.

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] qos apply policy policy_market inbound
[SwitchA-GigabitEthernet1/0/2] quit
```

Configuring Switch B to mirror traffic from the Technical Department

1. Configure local mirroring on Switch B:

Create local mirroring group 1.

```
<SwitchB> system-view
[SwitchB] mirroring-group 1 local
```

Configure the mirroring group to monitor the incoming traffic of the port GigabitEthernet 1/0/1.

```
[SwitchB] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 inbound
```

Configure GigabitEthernet 1/0/2 as the monitor port of the mirroring group.

```
[SwitchB] mirroring-group 1 monitor-port GigabitEthernet 1/0/2
```

2. Configure an ACL to filter the outgoing traffic from the Technical Department in working hours:

Create a working hour range named **work-time**, in which the working hour is from 8:30 to 18:00 on working days.

```
[SwitchB] time-range work-time 8:30 to 18:00 working-day
```

Create ACL 2000, and configure a rule to permit packets from 10.1.1.1 in working hours on working days.

```
[SwitchB] acl number 2000
```

```
[SwitchB-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.0 time-range work-time
```

```
[SwitchB-acl-basic-2000] quit
```

Apply ACL 2000 to filter the outgoing traffic on GigabitEthernet 1/0/2.

```
[SwitchB] interface GigabitEthernet1/0/2
```

```
[SwitchB-GigabitEthernet1/0/2] packet-filter 2000 outbound
```

```
[SwitchB-GigabitEthernet1/0/2] quit
```

Verifying the configuration

```
# Display traffic mirroring information on Switch A.
```

```
[SwitchA] display qos policy interface

Interface: GigabitEthernet1/0/2

Direction: Inbound

Policy: policy_market
Classifier: classifier_market_mgr
  Operator: AND
  Rule(s) : If-match acl 3001
  Behavior: behavior_market_mgr
  Filter Enable: permit
Classifier: classifier_market
  Operator: AND
  Rule(s) : If-match acl 3000
  Behavior: behavior_market
  Mirror enable:
    Mirror type: interface
    Mirror destination: GigabitEthernet1/0/3

Interface: GigabitEthernet1/0/3

Direction: Outbound

Policy: policy_servers
Classifier: classifier_servers
  Operator: AND
  Rule(s) : If-match acl 2000
  Behavior: behavior_servers
  Mirror enable:
    Mirror type: interface
    Mirror destination: GigabitEthernet1/0/3

Interface: GigabitEthernet1/0/4

Direction: Inbound

Policy: policy_servers
Classifier: classifier_servers
  Operator: AND
  Rule(s) : If-match acl 2000
  Behavior: behavior_servers
  Mirror enable:
    Mirror type: interface
```

```

        Mirror destination: GigabitEthernet1/0/3
# Display information about mirroring group 1 on Switch B.
[SwitchB] display mirroring-group 1
mirroring-group 1:
  type: local
  status: active
  mirroring port:
    GigabitEthernet1/0/1  inbound
  monitor port: GigabitEthernet1/0/2

```

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```

#
  time-range work-time 08:30 to 18:00 working-day
#
acl number 2000
  rule 0 permit source 14.1.1.0 0.0.0.255
acl number 2001
  rule 0 permit source 14.1.1.10 0 time-range work-time
#
acl number 3000
  rule 0 permit tcp source 12.1.1.0 0.0.0.255 destination-port eq www
acl number 3001
  rule 0 permit tcp source 12.1.1.100 0 destination-port eq www
#
traffic classifier classifier_servers operator and
  if-match acl 2000
traffic classifier classifier_fileserver operator and
  if-match acl 2001
traffic classifier classifier_market operator and
  if-match acl 3000
traffic classifier classifier_market_mgr operator and
  if-match acl 3001
#
traffic behavior behavior_servers
  mirror-to interface GigabitEthernet1/0/3
traffic behavior behavior_fileserver
  filter deny
traffic behavior behavior_market
  mirror-to interface GigabitEthernet1/0/3
traffic behavior behavior_market_mgr
  filter permit
#
qos policy policy_fileserver

```

```

classifier classifier_fileserver behavior behavior_fileserver
qos policy policy_market
classifier classifier_market_mgr behavior behavior_market_mgr
classifier classifier_market behavior behavior_market
qos policy policy_servers
classifier classifier_servers behavior behavior_servers
#
interface GigabitEthernet1/0/2
port link-mode bridge
qos apply policy policy_market inbound
#
interface GigabitEthernet1/0/3
port link-mode bridge
qos apply policy policy_servers outbound
#
interface GigabitEthernet1/0/4
port link-mode bridge
qos apply policy policy_servers inbound

```

- Switch B:

```

#
mirroring-group 1 local
#
time-range work-time 08:30 to 18:00 working-day
#
acl number 2000
rule 0 permit source 10.1.1.1 0 time-range work-time
#
interface GigabitEthernet1/0/1
port link-mode bridge
mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
port link-mode bridge
packet-filter 2000 outbound
mirroring-group 1 monitor-port

```

MLD configuration examples

This chapter provides examples for configuring MLD to manage IPv6 multicast group membership.

General configuration restrictions and guidelines

When you configure MLD, follow these restrictions and guidelines:

- Do not enable MLD on a VLAN interface that is running a Layer 2 IPv6 multicast protocol.
- Do not enable MLD proxying on a VLAN interface that is enabled with MLD snooping.
- Do not enable MLD on an interface that is enabled with MLD proxying.

Example: Configuring IPv6 multicast group filters

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

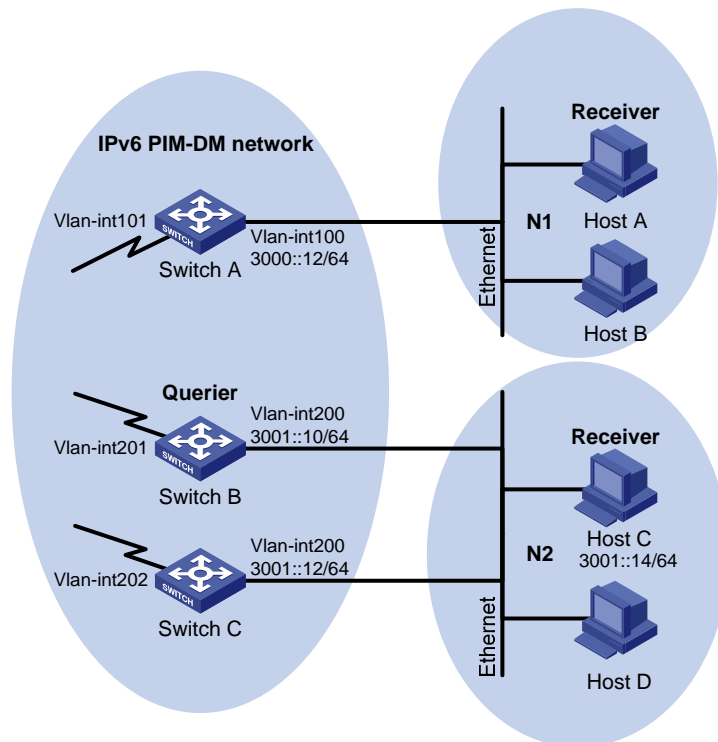
Network requirements

As shown in [Figure 122](#):

- 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 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 IPv6 multicast group FF1E::101. Hosts in N1 can join any IPv6 multicast group.

Figure 122 Network diagram



Requirements analysis

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, 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. Enable IPv6 forwarding and assign an IPv6 address to each interface of switches in the IPv6 PIM-DM domain, as shown in Figure 122. (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] multicast ipv6 routing-enable
# Enable MLD on VLAN-interface 100.
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
# Enable IPv6 PIM-DM on VLAN-interfaces 100 and 101.
[SwitchA-Vlan-interface100] pim ipv6 dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 dm
[SwitchA-Vlan-interface101] quit

```

4. Configure Switch B:

Create an ACL rule, and specify 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] multicast ipv6 routing-enable
```

Enable MLD and IPv6 PIM-DM on VLAN-interface 200.

```

[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] mld enable
[SwitchB-Vlan-interface200] pim ipv6 dm

```

Configure an IPv6 multicast group filter that references ACL 2001 on VLAN-interface 200.

```

[SwitchB-Vlan-interface200] mld group-policy 2001
[SwitchB-Vlan-interface200] quit

```

Enable IPv6 PIM-DM on VLAN-interface 201.

```

[SwitchB] interface vlan-interface 201
[SwitchB-Vlan-interface201] pim ipv6 dm
[SwitchB-Vlan-interface201] quit

```

5. Configure Switch C:

Create an ACL rule, and specify 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] multicast ipv6 routing-enable
```

Enable MLD and IPv6 PIM-DM on VLAN-interface 200.

```

[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] mld enable

```

```
[SwitchC-Vlan-interface200] pim ipv6 dm
# Configure an IPv6 multicast group filter that references ACL 2001 on VLAN-interface 200.
[SwitchC-Vlan-interface200] mld group-policy 2001
[SwitchC-Vlan-interface200] quit
# Enable IPv6 PIM-DM on VLAN-interface 202.
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] pim ipv6 dm
[SwitchC-Vlan-interface202] quit
```

Verifying the configuration

1. Display information about the MLD querier in N2:

Display information about the MLD querier on Switch B.

```
[SwitchB] display mld interface
Interface information of VPN-Instance: public net
Vlan-interface200(FE80::223:89FF:FE5F:958B):
  MLD is enabled
  Current MLD version is 1
  Value of query interval for MLD(in seconds): 125
  Value of other querier present interval for MLD(in seconds): 255
  Value of maximum query response time for MLD(in seconds): 10
  Querier for MLD: FE80::223:89FF:FE5F:958B (this router)
  Total 1 MLD Group reported
```

Display information about the MLD querier on Switch C.

```
[SwitchC] display mld interface
Interface information of VPN-Instance: public net
Vlan-interface200(FE80::223:89FF:FE5F:958C):
  MLD is enabled
  Current MLD version is 1
  Value of query interval for MLD(in seconds): 125
  Value of other querier present interval for MLD(in seconds): 255
  Value of maximum query response time for MLD(in seconds): 10
  Querier for MLD: FE80::223:89FF:FE5F:958B
  Total 1 MLD Group reported
```

The output shows that Switch B, with the smaller IPv6 link-local address, has become the MLD querier on this media-shared subnet.

2. Send MLD reports from Host C in N2 to join IPv6 multicast groups **FF1E::101** and **FF1E::102**. (Details not shown.)
3. Display information about MLD groups:

Display information about MLD groups on Switch B.

```
[SwitchB] display mld group
Total 1 MLD Group(s).
Interface group report information of VPN-Instance: public net
Vlan-interface200(FE80::223:89FF:FE5F:958B):
```

```

Total 1 MLD Group reported
Group Address: FF1E::101
Last Reporter: FE80::10
Uptime: 00:01:05
Expires: 00:03:17

# Display information about MLD groups on Switch C.
[SwitchC] display mld group
Total 1 MLD Group(s).
Interface group report information of VPN-Instance: public net
Vlan-interface200(FE80::223:89FF:FE5F:958C):
Total 1 MLD Group reported
Group Address: FF1E::101
Last Reporter: FE80::10
Uptime: 00:00:08
Expires: 00:01:12

```

The output shows that only information about the IPv6 multicast group FF1E::101 is displayed on Switch B and Switch C. The configured IPv6 multicast group filters have taken effect, and hosts in N2 can join only the IPv6 multicast group FF1E::101.

Configuration files

- Switch A:

```

#
 ipv6
#
 multicast ipv6 routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
 mld enable
 pim ipv6 dm
#
interface Vlan-interface101
 pim ipv6 dm
#

```
- Switch B:

```

#
 ipv6
#
 multicast ipv6 routing-enable
#
acl ipv6 number 2001
 rule 0 permit source FF1E::101/128
#
vlan 200 to 201

```

- ```

#
interface Vlan-interface200
 mld enable
 mld group-policy 2001
 pim ipv6 dm
#
interface Vlan-interface201
 pim ipv6 dm
#

```
- Switch C:

```

#
 ipv6
#
 multicast ipv6 routing-enable
#
 acl ipv6 number 2001
 rule 0 permit source FF1E::101/128
#
 vlan 200
#
 vlan 202
#
 interface Vlan-interface200
 mld enable
 mld group-policy 2001
 pim ipv6 dm
#
 interface Vlan-interface202
 pim ipv6 dm
#

```

## Example: Configuring MLD SSM mappings

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

### Network requirements

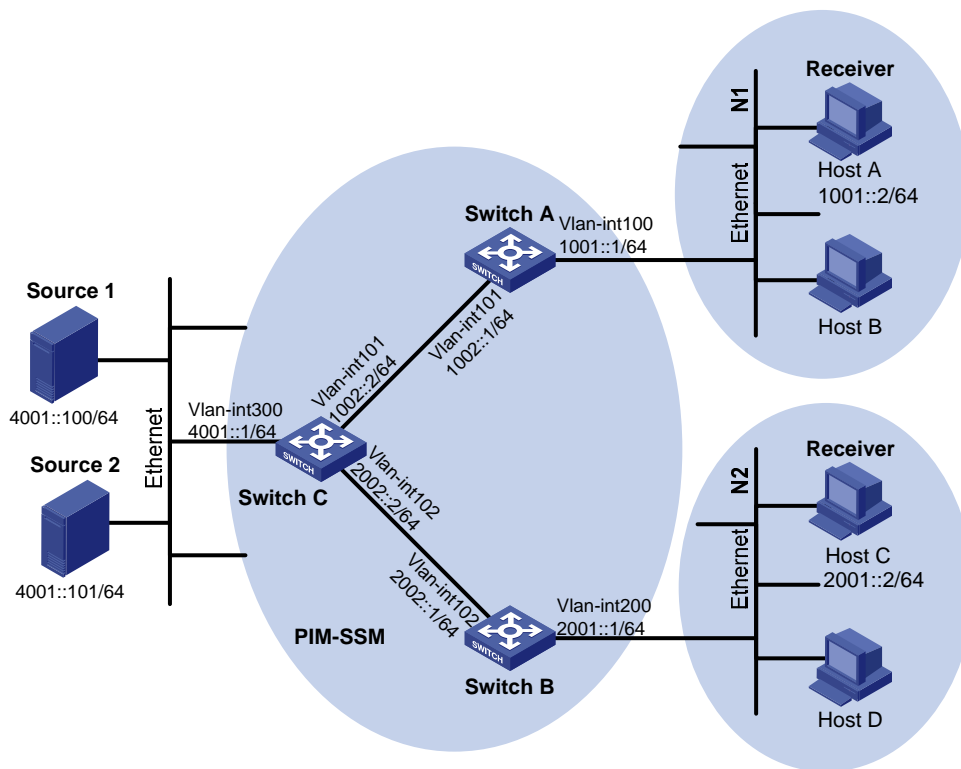
As shown in [Figure 123](#):

- The IPv6 PIM-SSM network provides services for the IPv6 multicast groups in the range of FF3E::/64.

- Edge switches of N1 and N2 are running MLDv2.
- Host A and Host C support MLDv1, but do not support MLDv2.
- All switches run OSPF, and they can communicate with each other through unicast routes.

Configure MLD SSM mappings so that Host A and Host C receive IPv6 multicast data from Source 1 and Source 2, respectively.

**Figure 123 Network diagram**



## Configuration restrictions and guidelines

When you configure MLD SSM mapping, follow these restrictions and guidelines:

- The MLD SSM mapping does not process MLDv2 reports.
- To display information about the IPv6 multicast groups created based on the configured MLD SSM mappings, use the **display mld ssm-mapping group** command. Do not use the **display mld group** command.

## Configuration procedures

1. Enable IPv6 forwarding on each switch and assign an IPv6 address to each interface of switches as shown in [Figure 123](#). (Details not shown.)
2. Enable OSPFv3 on all switches on the IPv6 PIM-SM network. (Details not shown.)

3. Enable IPv6 multicast routing and IPv6 PIM-SM:

# On Switch A, enable IPv6 multicast routing and enable IPv6 PIM-SM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
[SwitchA-Vlan-interface101] quit
```

# Enable IPv6 multicast routing and IPv6 PIM-SM on Switch B and Switch C in the same way Switch A is configured. (Details not shown.)

4. Enable MLDv2 on interfaces that connect N1 and N2:

# Enable MLDv2 on VLAN-interface 100 of Switch A. (By default, the MLD version is 1.)

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] mld version 2
[SwitchA-Vlan-interface100] quit
```

# Enable MLDv2 on Switch B in the same way Switch A is configured. (Details not shown.)

5. Specify the IPv6 SSM multicast group address range:

# On Switch A, specify the IPv6 SSM multicast group address range as FF3E::/64.

```
[SwitchA] acl ipv6 number 2000
[SwitchA-acl6-basic-2000] rule permit source ff3e:: 64
[SwitchA-acl6-basic-2000] quit
[SwitchA] pim ipv6
[SwitchA-pim6] ssm-policy 2000
[SwitchA-pim6] quit
```

# Specify the same IPv6 SSM multicast group address range on Switch B and Switch C in the same way Switch A is configured. (Details not shown.)

6. Enable MLD SSM mapping and configure MLD SSM mappings:

# On Switch A, enable MLD SSM mapping on VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld ssm-mapping enable
[SwitchA-Vlan-interface100] quit
```

# Configure an MLD SSM mapping for the IPv6 multicast source (Source 1) and IPv6 multicast groups in the range of **FF3E::/64**.

```
[SwitchA] mld
[SwitchA-mld] ssm-mapping ff3e:: 64 4001::100
[SwitchA-mld] quit
```

# On Switch B, enable MLD SSM mapping on VLAN-interface 200.

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] mld ssm-mapping enable
[SwitchB-Vlan-interface200] quit
```

# Configure an MLD SSM mapping for the IPv6 multicast source (Source 2) and IPv6 multicast groups in the range of **FF3E::/64**.

```
[SwitchB] mld
[SwitchB-mld] ssm-mapping ff3e:: 64 4001::101
[SwitchB-mld] quit
```

## Verifying the configuration

1. Send MLDv1 reports from Host A and Host C to join the IPv6 multicast group **FF3E::101**. (Details not shown.)
2. Display IPv6 multicast information on Switch A:

# Display the MLD SSM mapping information of the IPv6 multicast group FF3E::101.

```
[SwitchA] display mld ssm-mapping ff3e::101
VPN-Instance: public net
Group: FF3E::101
Source list:
4001::100
```

# Display information about the IPv6 multicast group created based on the configured MLD SSM mapping.

```
[SwitchA] display mld ssm-mapping group
Total 1 MLD SSM-mapping Group(s).
Interface group report information of VPN-Instance: public net
Vlan-interface100(FE80::223:89FF:FE5F:958A):
Total 1 MLD SSM-mapping Group reported
Group Address: FF3E::101
Last Reporter: FE80::10
Uptime: 00:02:04
Expires: off
```

# Display the IPv6 PIM routing table.

```
[SwitchA] display pim ipv6 routing-table
VPN-Instance: public net
Total 1 (S, G) entry

(4001::100, FF3E::101)
Protocol: pim-ssm, Flag:
UpTime: 00:13:25
Upstream interface: Vlan-interface101
Upstream neighbor: FE80::223:89FF:FE5F:958C
RPF prime neighbor: FE80::223:89FF:FE5F:958C
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface100
Protocol: mld, UpTime: 00:13:25, Expires: -
```

3. Display IPv6 multicast information on Switch B:



# Display the MLD SSM mapping information of the IPv6 multicast group FF3E::101.

```
[SwitchB] display mld ssm-mapping ff3e::101
VPN-Instance: public net
Group: FF3E::101
Source list:
4001::101
```

# Display information about the IPv6 multicast group created based on the configured MLD SSM mapping.

```
[SwitchB] display mld ssm-mapping group
Total 1 MLD SSM-mapping Group(s).
Interface group report information of VPN-Instance: public net
Vlan-interface200(FE80::223:89FF:FE5F:958B):
Total 1 MLD SSM-mapping Group reported
Group Address: FF3E::101
Last Reporter: FE80::13
Uptime: 00:01:26
Expires: off
```

# Display the IPv6 PIM routing table.

```
[SwitchB] display pim ipv6 routing-table
VPN-Instance: public net
Total 1 (S, G) entry

(4001::101, FF3E::101)
Protocol: pim-ssm, Flag:
UpTime: 00:12:16
Upstream interface: Vlan-interface102
Upstream neighbor: FE80::223:89FF:FE5F:958C
RPF prime neighbor: FE80::223:89FF:FE5F:958C
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface200
Protocol: mld, UpTime: 00:05:21, Expires: -
```

The output shows that:

- After an MLD SSM mapping is configured on Switch A, Switch A translates (::,FF3E::101) into (4001::100, FF3E::101). Host A can receive IPv6 multicast data only from Source 1.
- After an MLD SSM mapping is configured on Switch B, Switch B translates (::,FF3E::101) into (4001::100, FF3E::101). Host C can receive IPv6 multicast data only from Source 2.

## Configuration files

- Switch A:

```
#
ipv6
#
multicast ipv6 routing-enable
```

```

#
acl ipv6 number 2000
 rule 0 permit source FF3E::/64
#
vlan 100 to 101
#
interface Vlan-interface100
 ipv6 address 1001::1/64
 ospfv3 1 area 0.0.0.0
 mld enable
 mld version 2
 mld ssm-mapping enable
 pim ipv6 sm
#
interface Vlan-interface101
 ipv6 address 1002::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
ospfv3 1
 router-id 1.1.1.1
 area 0.0.0.0
#
mld
 ssm-mapping ff3e:: 64 4001::100
#
pim ipv6
 ssm-policy 2000
#

```

- **Switch B:**

```

#
ipv6
#
multicast ipv6 routing-enable
#
acl ipv6 number 2000
 rule 0 permit source FF3E::/64
#
vlan 102
#
vlan 200
#
interface Vlan-interface102
 ipv6 address 2002::1/64
 ospfv3 1 area 0.0.0.0
 pim ipv6 sm
#
interface Vlan-interface200

```

```

ipv6 address 2001::1/64
ospfv3 1 area 0.0.0.0
mld enable
mld version 2
mld ssm-mapping enable
pim ipv6 sm
#
ospfv3 1
router-id 2.2.2.2
area 0.0.0.0
#
mld
ssm-mapping ff3e:: 64 4001::101
#
pim ipv6
ssm-policy 2000
#

```

- Switch C:

```

#
ipv6
#
multicast ipv6 routing-enable
#
acl ipv6 number 2000
rule 0 permit source FF3E::/64
#
vlan 101 to 102
#
vlan 300
#
interface Vlan-interface101
ipv6 address 1002::2/64
ospfv3 1 area 0.0.0.0
pim ipv6 sm
#
interface Vlan-interface102
ipv6 address 2002::2/64
ospfv3 1 area 0.0.0.0
pim ipv6 sm
#
interface Vlan-interface300
ipv6 address 4001::1/64
ospfv3 1 area 0.0.0.0
pim ipv6 sm
#
ospfv3 1
router-id 3.3.3.3
area 0.0.0.0

```

```

#
pim ipv6
 ssm-policy 2000
#

```

## Example: Configuring MLD proxying

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

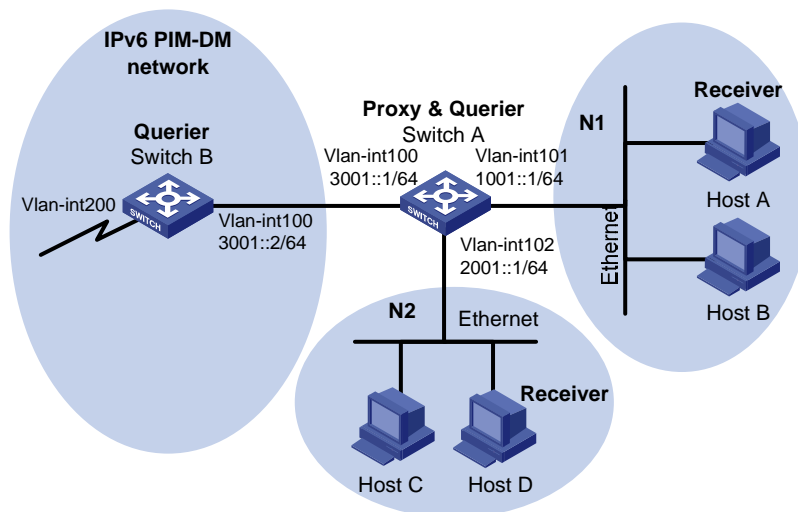
### Network requirements

As shown in [Figure 124](#):

- User networks N1 and N2 connect to the MLD querier (Switch B) in the IPv6 PIM-DM domain through a Layer 3 switch (Switch A).
- All switches run OSPF, and they can communicate with each other through unicast routes.

Configure MLD proxying on Switch A, so that the receiver hosts in N1 and N2 can receive IPv6 multicast data from the IPv6 PIM-DM domain even though Switch A is not running IPv6 PIM-DM.

**Figure 124 Network diagram**



### Requirements analysis

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

- Enable MLD proxying on the upstream interface of Switch A.
- Enable MLD on the downstream interface of Switch A.

## Configuration restrictions and guidelines

When you configure MLD proxying, follow these restrictions and guidelines:

- Enable IPv6 multicast routing before you enable MLD proxying.
- Only one interface on a device can be enabled with MLD proxying.

## Configuration procedures

1. Enable IPv6 forwarding on each switch and assign an IPv6 address to each interface of switches, as shown in [Figure 124](#). (Details not shown.)

2. Configure Switch A:

```
Enable IPv6 multicast routing globally.
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable

Enable MLD proxying on VLAN-interface 100.
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface102] mld proxying enable
[SwitchA-Vlan-interface102] quit

Enable MLD on VLAN-interface 101 and VLAN-interface 102.
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] mld enable
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] mld enable
[SwitchA-Vlan-interface102] quit
```

3. Configure Switch B:

```
Enable IPv6 multicast routing globally.
<SwitchB> system-view
[SwitchB] multicast ipv6 routing-enable

Enable PIM-DM on each interface.
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] pim ipv6 dm
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] pim ipv6 dm
[SwitchB-Vlan-interface200] quit

Enable MLD on VLAN-interface 100.
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] mld enable
```

```
[SwitchB-Vlan-interface100] quit
```

## Verifying the configuration

1. Send an MLD report from Host A in N1 to join IPv6 multicast group **FF1E::101**. (Details not shown.)
2. Display MLD group information on Switch A and Switch B:

```
Display MLD group information of VLAN-interface 101 on Switch A.
```

```
[SwitchA] display mld group interface vlan-interface 101
```

```
Vlan-interface101(FE80::20F:E2FF:FE67:B323):
```

```
Total 1 MLD Group reported
```

| Group Address | Last Reporter | Uptime   | Expires  |
|---------------|---------------|----------|----------|
| FF1E::101     | FE80::10      | 00:10:14 | 00:01:10 |

The output shows that Switch A creates and maintains group membership for the IPv6 multicast group FF1E::101 after it receives the report on VLAN-interface 101. Switch A acts as an MLD router from the perspective of downstream hosts.

```
Display MLD group information of VLAN-interface 100 on Switch B.
```

```
[SwitchB] display mld group interface Vlan-interface 102
```

```
Vlan-interface100(FE80::2E0:FCFF:FE66:5502):
```

```
Total 1 MLD Group reported
```

| Group Address | Last Reporter            | Uptime   | Expires  |
|---------------|--------------------------|----------|----------|
| FF1E::101     | FE80::20F:E2FF:FE67:B323 | 00:11:14 | 00:01:58 |

The output shows that Switch B creates and maintains group membership for the IPv6 multicast group FF1E::101 after it receives the report from Switch A on VLAN-interface 100. Switch A acts as a receiver host from the perspective of Switch B.

## Configuration files

- Switch A:

```
#
ipv6
#
multicast ipv6 routing-enable
#
vlan 100 to 102
#
interface Vlan-interface100
mld enable
#
interface Vlan-interface101
mld enable
#
interface Vlan-interface102
mld proxying enable
#
```

- Switch B:

```
#
 ipv6
#
 multicast ipv6 routing-enable
#
vlan 100
#
vlan 200
#
interface Vlan-interface102
 mld enable
 pim ipv6 dm
#
interface Vlan-interface103
 pim ipv6 dm
#
```

# MLD snooping configuration examples

This chapter provides examples for configuring MLD snooping to manage and control IPv6 multicast group forwarding at Layer 2.

## General configuration restrictions and guidelines

Do not enable MLD snooping on a VLAN if the VLAN interface is running a Layer 3 multicast protocol.

## Example: Configuring an MLD snooping multicast group filter

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

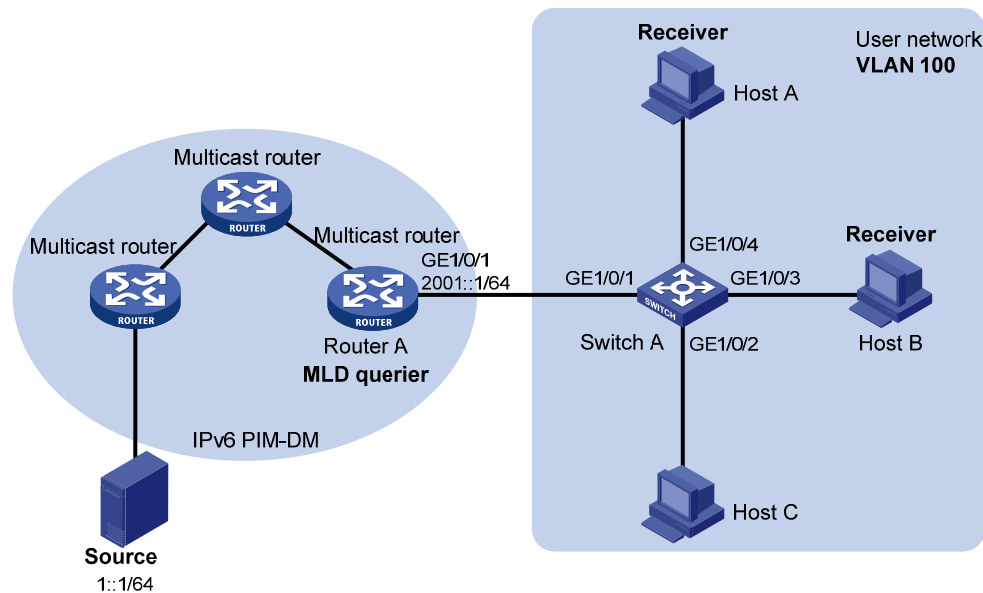
As shown in [Figure 125](#):

- 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 IPv6 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 125 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 ACL, specifying the range of the 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 if it has no rule, the filter will filter out all multicast groups.

## Configuration procedures

```
Enable IPv6 forwarding on the switch. (Details not shown.)
```

```
Enable MLD snooping globally.
```

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

```
Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN.
```

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

```
Enable 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 to permit the IPv6 multicast group FF1E::101.
[SwitchA] acl ipv6 number 2001
[SwitchA-acl6-basic-2001] rule permit source ff1e::101 128
[SwitchA-acl6-basic-2001] quit

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

1. Send MLD reports from Host A and Host B to join the IPv6 multicast groups **FF1E::101** and **FF1E::102**, respectively. (Details not shown.)
2. Display detailed MLD snooping group information on Switch A.

```
[SwitchA] display mld-snooping group verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port.
 GE1/0/1 (D)
IP group(s):the following ip group(s) match to one mac group.
IP group address:FF1E::101
 (::, FF1E::101):
 Attribute: Host Port
 Host port(s):total 1 port.
 GE1/0/4 (D)
MAC group(s):
MAC group address: 3333-0000-0101
Host port(s):total 1 port.
 GE1/0/4
```

The output shows that Switch A has only the entry for IPv6 multicast group FF1E::101. The configured IPv6 multicast group filter is functioning.

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
 ipv6
#
acl ipv6 number 2001
 rule 0 permit source FF1E::101/128
#
 mld-snooping
 group-policy 2001 vlan 100
#
vlan 100
 mld-snooping enable
 mld-snooping drop-unknown
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#
```

## Example: Configuring MLD snooping static ports

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

# Network requirements

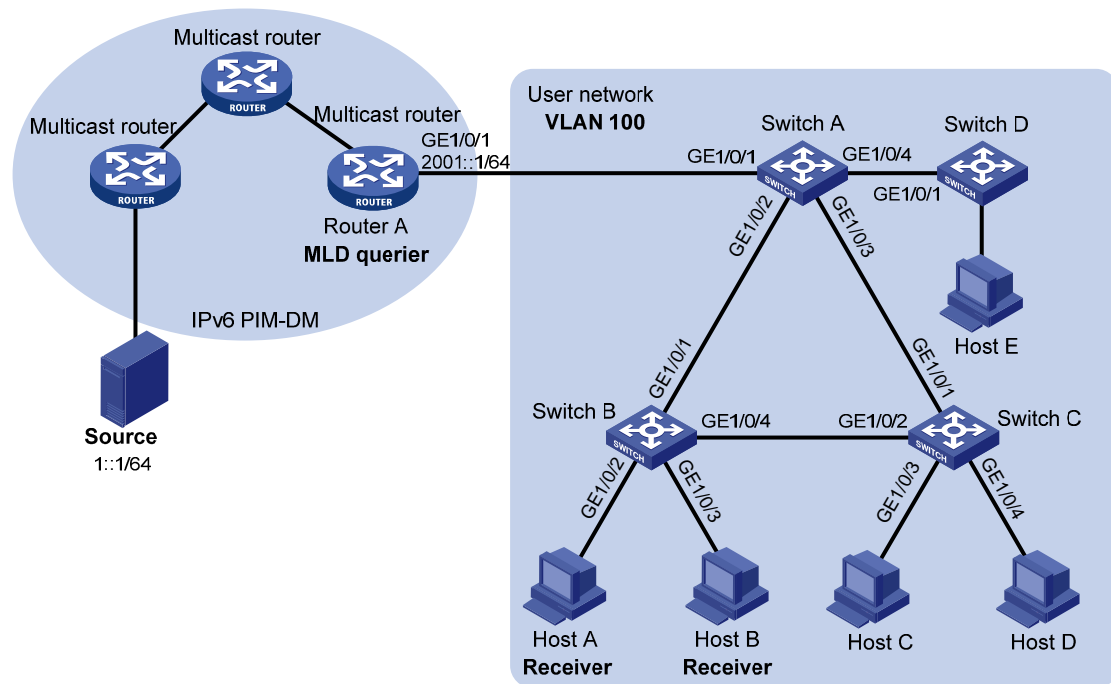
As shown in Figure 126:

- 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 IPv6 multicast source 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 immediately switch from one failed path between Switch A and Switch B to the other path after the new path comes up and becomes stable.

Figure 126 Network diagram



# Requirements analysis

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

- To make sure the receiver hosts receive multicast packets for a fixed IPv6 multicast group, configure the ports that are connected to the hosts as MLD snooping static member ports.

- 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 an immediate switchover to the new path, configure all ports that might become the outgoing ports as MLD snooping static router ports.

## Configuration procedures

1. Enable IPv6 forwarding on the switches. (Details not shown.)
2. Configure Switch A:

# Enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

# Enable MLD snooping for VLAN 100.

```
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] quit
```

# Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as MLD snooping static router ports.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] mld-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

3. Configure Switch B:

# Enable MLD snooping globally.

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

# Enable MLD snooping for VLAN 100.

```
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] quit
```

# Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as MLD snooping static member ports of the IPv6 multicast group FF1E::101.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] mld-snooping static-group ff1e::101 vlan 100
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] mld-snooping static-group ff1e::101 vlan 100
[SwitchB-GigabitEthernet1/0/3] quit
```

#### 4. Configure Switch C:

# Enable MLD snooping globally.

```
<SwitchC> system-view
[SwitchC] mld-snooping
[SwitchC-mld-snooping] quit
```

# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

# Enable MLD snooping for VLAN 100.

```
[SwitchC-vlan100] mld-snooping enable
[SwitchC-vlan100] quit
```

# Configure GigabitEthernet 1/0/2 as an MLD snooping static router port.

```
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] mld-snooping static-router-port vlan 100
[SwitchC-GigabitEthernet1/0/2] quit
```

## Verifying the configuration

1. Send MLD reports from Host A and Host B to join the IPv6 multicast group **FF1E::101**. (Details not shown.)
2. Display detailed MLD snooping group information for VLAN 100 on Switch A.

```
[SwitchA] display mld-snooping group vlan 100 verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 3 port.
 GE1/0/1 (D)
 GE1/0/2 (S)
 GE1/0/3 (S)

IP group(s):the following ip group(s) match to one mac group.
IP group address: FF1E::101
```

```
(::, FF1E::101):
 Attribute: Host Port
 Host port(s):total 1 port.
 GE1/0/2 (D)
MAC group(s):
 MAC group address:3333-0000-0101
 Host port(s):total 1 port.
 GE1/0/2
```

The output shows that GigabitEthernet 1/0/2 and GigabitEthernet1/0/3 on Switch A are MLD snooping static router ports.

### 3. Display detailed MLD snooping group information for VLAN 100 on Switch B.

```
[SwitchB] display mld-snooping group vlan 100 verbose
```

```
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
```

```
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
Vlan(id):100.
```

```
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
```

```
Router port(s):total 1 port.
```

```
 GE1/0/2 (D)
```

```
IP group(s):the following ip group(s) match to one mac group.
```

```
 IP group address: FF1E::101
```

```
(::, FF1E::101):
```

```
 Attribute: Host Port
```

```
 Host port(s):total 2 port.
```

```
 GE1/0/2 (S)
```

```
 GE1/0/3 (S)
```

```
MAC group(s):
```

```
 MAC group address:3333-0000-0101
```

```
 Host port(s):total 2 port.
```

```
 GE1/0/2
```

```
 GE1/0/3
```

The output shows that GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 on Switch B are MLD snooping static router ports for the IPv6 multicast group.

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```
#
 ipv6
#
```

```

mld-snooping
#
vlan 100
 mld-snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 mld-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
 mld-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#

```

- Switch B:

```

#
 ipv6
#
 mld-snooping
#
vlan 100
 mld-snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 mld-snooping static-group ffile::101 vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
 mld-snooping static-group ffile::101 vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge

```



```

 port access vlan 100
#
• Switch C:
#
 ipv6
#
 mld-snooping
#
vlan 100
 mld-snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 mld-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#

```

## Example: Configuring an MLD snooping querier

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

### Network requirements

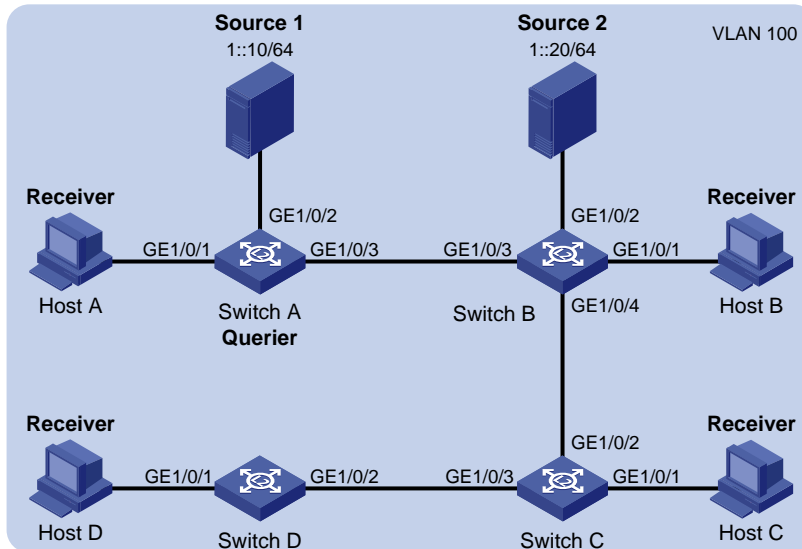
As shown in [Figure 127](#):

- The network is a Layer 2-only network.
- Source 1 and Source 2 send multicast packets to the multicast groups FF1E::101 and FF1E::102, respectively.

- Host A and Host C are receivers of multicast group FF1E::101, and Host B and Host D are receivers of multicast group FF1E::102.

Configure an MLD snooping querier so the receiver hosts receive their expected multicast packets.

**Figure 127 Network diagram**



## Requirements analysis

To establish and maintain Layer 2 multicast forwarding entries, configure the switch that is close to the multicast sources (Switch A in this example) as the MLD snooping querier.

## Configuration procedures

1. Enable IPv6 forwarding on each switch. (Details not shown.)
2. Configure Switch A:

# Enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to this VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

# Enable MLD snooping and the MLD snooping querier feature for VLAN 100.

```
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping querier
[SwitchA-vlan100] quit
```

### 3. Configure Switch B:

# Enable MLD snooping globally.

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

# Enable MLD snooping for VLAN 100.

```
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] quit
```

### 4. Configure Switch C and Switch D in the same way Switch B is configured. (Details not shown.)

## Verifying the configuration

# Display statistics for MLD packets that have been received on Switch B.

```
[SwitchB-vlan100] display mld-snooping statistics
Received MLD general queries:96.
Received MLDv1 specific queries:0.
Received MLDv1 reports:105.
Received MLD dones:0.
Sent MLDv1 specific queries:0.
Received MLDv2 reports:0.
Received MLDv2 reports with right and wrong records:0.
Received MLDv2 specific queries:0.
Received MLDv2 specific sg queries:0.
Sent MLDv2 specific queries:0.
Sent MLDv2 specific sg queries:0.
Received error MLD messages:0.
```

The output shows that the configured MLD snooping querier has successfully sent MLD queries.

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```
#
ipv6
#
mld-snooping
#
vlan 100
mld-snooping enable
mld-snooping querier
```

```

#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#

```

- **Switch B:**

```

#
 ipv6
#
 mld-snooping
#
vlan 100
 mld-snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#

```

- **Switch C and Switch D:**

The configuration information on Switch C and Switch D is similar to that on Switch B. (Details not shown.)

# Example: Configuring MLD snooping proxying

## Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

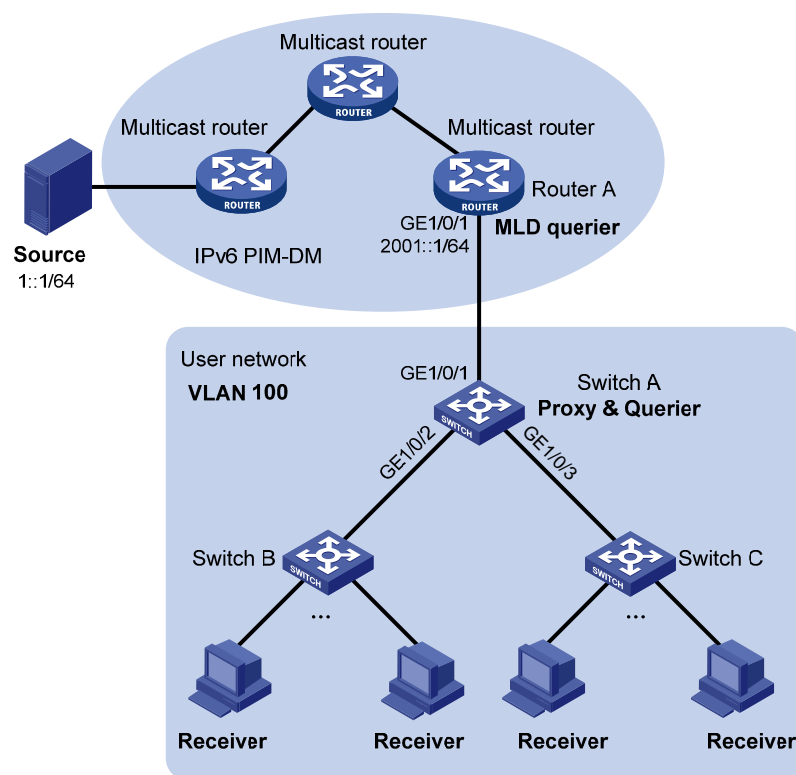
## Network requirements

As shown in [Figure 128](#):

- The user network VLAN 100 is connected to the MLD querier (Router A) in the IPv6 PIM-DM domain through Switch A.
- MLD snooping is enabled on all switches in VLAN 100.
- Many receivers in VLAN 100 frequently join or leave the multicast group, sending large amounts of MLD reports and done messages to the MLD querier.

Configure an MLD snooping proxy to reduce the burden on the MLD querier.

**Figure 128 Network diagram**



## Requirements analysis

To reduce the number of MLD report and done messages received by upstream devices, enable MLD snooping proxying on the device that is closest to the MLD querier (Switch A in this example).

## Configuration restrictions and guidelines

Before configuring MLD snooping proxying, enable MLD snooping globally and for the specified VLANs.

## Configuration procedures

1. Enable IPv6 forwarding on each switch. (Details not shown.)
2. Configure Switch A:

```
Enable MLD snooping globally.
```

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

```
Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to this VLAN.
```

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

```
Enable MLD snooping and MLD snooping proxying for VLAN 100.
```

```
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping proxying enable
```

```
Configure the source IPv6 addresses for the proxy to use for MLD reports and done messages.
```

```
[SwitchA-vlan100] mld-snooping report source-ip fe80:0:0:1::1
[SwitchA-vlan100] mld-snooping done source-ip fe80:0:0:1::1
[SwitchA-vlan100] quit
```

3. Configure Switch B and Switch C:

Create VLAN 100, and assign ports that are connected to the receiver hosts to the VLAN. Enable MLD snooping for the VLAN. (Details not shown.)

## Verifying the configuration

1. Send MLD reports from the hosts in the user network to join the IPv6 multicast group **FF1E::101**. (Details not shown.)
2. Display MLD multicast group information on Router A.

```
[RouterA] display mld group
Total 1 MLD Group(s).
```

```
Interface group report information of VPN-Instance: public net
GigabitEthernet1/0/1(FE80::200:FCFF:FE00:7507):
 Total 1 MLD Group reported
 Group Address: FF1E::101
 Last Reporter: FE80:0:0:1::1
 Uptime: 00:00:03
 Expires: 00:04:17
```

The output shows that the last reporter address is the source IPv6 address that you configure for the MLD snooping proxy to use for MLD reports. Switch A has sent MLD reports to the MLD querier on behalf of receiver hosts.

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
ipv6
#
mld-snooping
#
vlan 100
 mld-snooping enable
 mld-snooping proxying enable
 mld-snooping report source-ip fe80:0:0:1::1
 mld-snooping done source-ip fe80:0:0:1::1
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
```

# Multicast VLAN configuration examples

This document provides examples for configuring multicast VLANs to reduce the traffic load on Layer 3 devices.

Multicast VLANs include sub-VLAN-based multicast VLANs and port-based multicast VLANs.

- In a sub-VLAN-based multicast VLAN, IGMP snooping manages router ports in the multicast VLAN and user ports in each sub-VLAN. It is applicable to all networking environments.
- In a port-based multicast VLAN, IGMP snooping manages the router ports and user ports in the multicast VLAN. Port-based multicast VLANs are typically deployed on devices that are directly connected to receivers. Port-based multicast VLANs are easier to implement than sub-VLAN-based multicast VLANs.

## General configuration restrictions and guidelines

When you configure multicast VLANs, follow these restrictions and guidelines:

- Do not configure multicast VLAN on a device with multicast routing enabled.
- The port-based multicast VLAN takes precedence over the sub-VLAN-based multicast VLAN if they are both configured on a device.

## Example: Configuring a sub-VLAN-based multicast VLAN

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

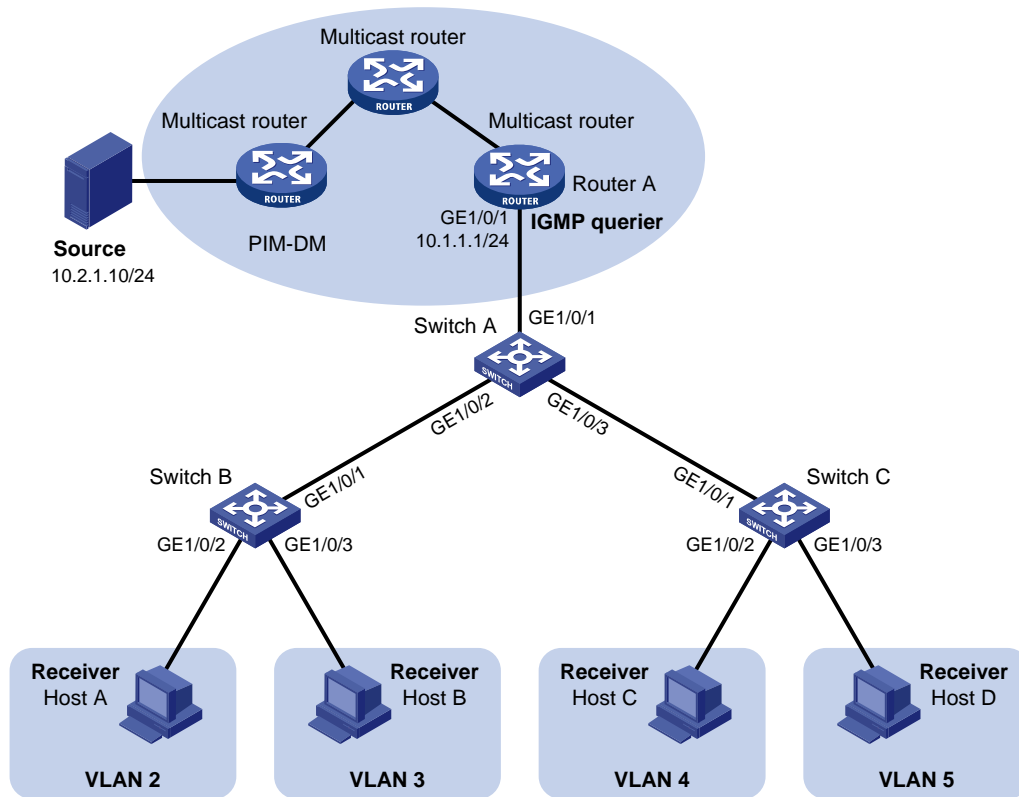
As shown in [Figure 129](#):

- The Layer 2 user network is connected to the IGMP querier (Router A) in the PIM-DM domain through Switch A.
- Each user VLAN has a receiver host that belongs to the same multicast group.



To save bandwidth and reduce the burden on Layer 3 multicast routers, configure a sub-VLAN-based multicast VLAN on Switch A. In this scenario, Layer 3 multicast routers only need to forward multicast data to the multicast VLAN. Receiver hosts in different user VLANs can receive the data.

**Figure 129 Network diagram**



## Configuration restrictions and guidelines

When you configure a sub-VLAN-based multicast VLAN, follow these restrictions and guidelines:

- The VLAN to be configured as a multicast VLAN must exist.
- The VLAN to be configured as a sub-VLAN must exist and cannot be a multicast VLAN or a sub-VLAN of any other multicast VLANs.
- After you enable IGMP snooping for the multicast VLAN, the sub-VLANs are automatically enabled with IGMP snooping.

## Configuration procedures

### Configuring Switch A

# Enable IGMP snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
```

```

[SwitchA-igmp-snooping] quit

Create VLAN 2 through VLAN 5. Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to
VLAN 2 and VLAN 3.
[SwitchA] vlan 2 to 5
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 2 3
[SwitchA-GigabitEthernet1/0/2] quit

Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLAN 4 and VLAN 5.
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 4 5
[SwitchA-GigabitEthernet1/0/3] quit

Create VLAN 1024, and assign GigabitEthernet 1/0/1 to this VLAN.
[SwitchA] vlan 1024
[SwitchA-vlan1024] port gigabitethernet 1/0/1

Enable IGMP snooping for VLAN 1024.
[SwitchA-vlan1024] igmp-snooping enable
[SwitchA-vlan1024] quit

Configure VLAN 1024 as the multicast VLAN.
[SwitchA] multicast-vlan 1024

Configure VLAN 2 through VLAN 5 as the sub-VLANs.
[SwitchA-mvlan-1024] subvlan 2 to 5

```

## Configuring Switch B

```

Enable IGMP snooping globally.
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit

Create VLAN 2, and assign GigabitEthernet 1/0/2 to this VLAN.
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/2

Enable IGMP snooping for VLAN 1024.
[SwitchB-vlan2] igmp-snooping enable
[SwitchB-vlan2] quit

Configure VLAN 3, and assign GigabitEthernet 1/0/3 to this VLAN.
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/3

Enable IGMP snooping for VLAN 3.
[SwitchB-vlan3] igmp-snooping enable
[SwitchB-vlan3] quit

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLAN 2 and VLAN 3.

```

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2 3
```

## Configuring Switch C

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

## Verifying the configuration

1. Send IGMP reports from the receiver hosts in the user VLANs to join the multicast group **224.1.1.1**. (Details not shown.)
2. Verify that Switch A can receive the reports and that it can forward the reports to Router A.

# Display information about the multicast VLAN on Switch A.

```
[SwitchA] display multicast-vlan
Total 1 multicast-vlan(s)
```

```
Multicast vlan 1024
```

```
subvlan list:
```

```
vlan 2-5
```

```
port list:
```

```
no port
```

# Display IGMP snooping group information on Switch A.

```
[SwitchA] display igmp-snooping group
```

```
Total 5 IP Group(s).
```

```
Total 5 IP Source(s).
```

```
Total 5 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
```

```
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
Vlan(id):2.
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Router port(s):total 0 port.
```

```
IP group(s):the following ip group(s) match to one mac group.
```

```
IP group address:224.1.1.1
```

```
(0.0.0.0, 224.1.1.1):
```

```
Host port(s):total 1 port.
```

```
GE1/0/2 (D)
```

```
MAC group(s):
```

```
MAC group address:0100-5e01-0101
```

```
Host port(s):total 1 port.
```

```
GE1/0/2
```

```
Vlan(id):3.
```

```
Total 1 IP Group(s).
```

Total 1 IP Source(s).

Total 1 MAC Group(s).

Router port(s):total 0 port.

IP group(s):the following ip group(s) match to one mac group.

IP group address:224.1.1.1

(0.0.0.0, 224.1.1.1):

Host port(s):total 1 port.

GE1/0/2 (D)

MAC group(s):

MAC group address:0100-5e01-0101

Host port(s):total 1 port.

GE1/0/2

Vlan(id):4.

Total 1 IP Group(s).

Total 1 IP Source(s).

Total 1 MAC Group(s).

Router port(s):total 0 port.

IP group(s):the following ip group(s) match to one mac group.

IP group address:224.1.1.1

(0.0.0.0, 224.1.1.1):

Host port(s):total 1 port.

GE1/0/3 (D)

MAC group(s):

MAC group address:0100-5e01-0101

Host port(s):total 1 port.

GE1/0/3

Vlan(id):5.

Total 1 IP Group(s).

Total 1 IP Source(s).

Total 1 MAC Group(s).

Router port(s):total 0 port.

IP group(s):the following ip group(s) match to one mac group.

IP group address:224.1.1.1

(0.0.0.0, 224.1.1.1):

Host port(s):total 1 port.

GE1/0/3 (D)

MAC group(s):

MAC group address:0100-5e01-0101

Host port(s):total 1 port.

GE1/0/3

Vlan(id):1024.

Total 1 IP Group(s).

Total 1 IP Source(s).

Total 1 MAC Group(s).

Router port(s):total 1 port.

```

GE1/0/1 (D)
IP group(s):the following ip group(s) match to one mac group.
IP group address:224.1.1.1
(0.0.0.0, 224.1.1.1):
Host port(s):total 0 port.
MAC group(s):
MAC group address:0100-5e01-0101
Host port(s):total 0 port.

```

The output shows that:

- IGMP snooping in the multicast VLAN (VLAN 1024) maintains the router ports.
- IGMP snooping in the sub-VLANs (VLAN 2 through VLAN 5) maintains the member ports.

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```

#
igmp-snooping
#
vlan 2 to 5
#
vlan 1024
igmp-snooping enable
#
multicast-vlan 1024
subvlan 2 to 5
#
interface GigabitEthernet1/0/1
port link-mode bridge
port access vlan 1024
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 3
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
port trunk permit vlan 4 to 5
#

```

# Example: Configuring a port-based multicast VLAN

## Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

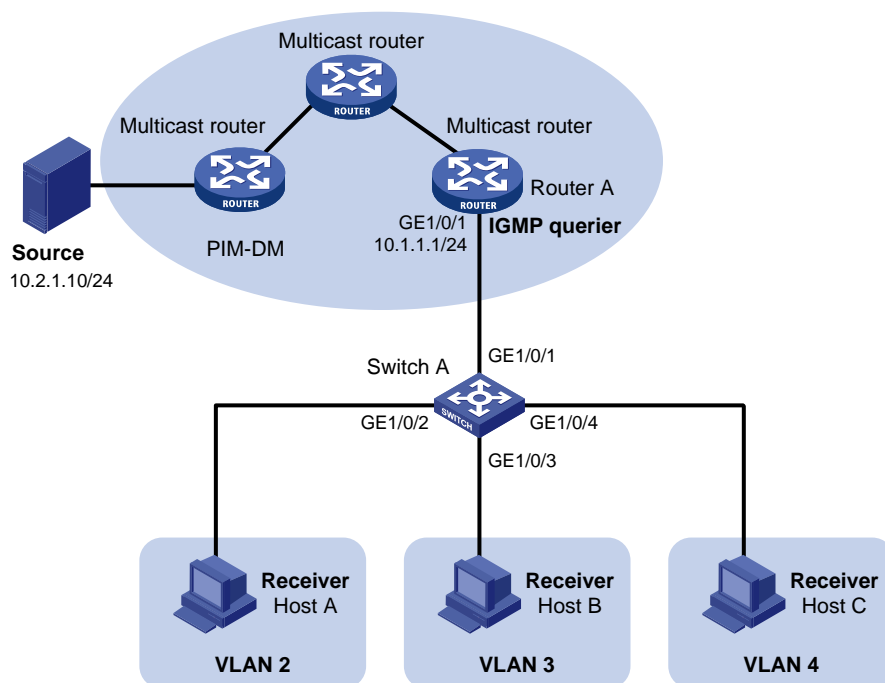
## Network requirements

As shown in [Figure 130](#):

- The Layer 2 user network is connected to the IGMP querier (Router A) in the PIM-DM domain through Switch A.
- Each user VLAN has a receiver host that belongs to the same multicast group, and the receiver hosts are directly connected to Switch A.

To save bandwidth and reduce the burden on Layer 3 multicast routers, configure a port-based multicast VLAN on Switch A. In this scenario, Layer 3 multicast routers only need to send multicast data to the multicast VLAN. Receiver hosts in different user VLANs can receive the data.

**Figure 130 Network diagram**



## Configuration restrictions and guidelines

When you configure a port-based multicast VLAN, follow these restrictions and guidelines:

- The VLAN to be configured as the multicast VLAN must exist.
- A port can belong to only one multicast VLAN.
- You must enable IGMP snooping for the multicast VLAN and the user VLANs.
- The user ports must be hybrid ports. You must assign user ports to the multicast VLAN and user VLANs as untagged VLAN members.

## Configuration procedures

**# Enable IGMP snooping globally.**

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

**# Create VLAN 1024, and assign GigabitEthernet 1/0/1 to this VLAN.**

```
[SwitchA] vlan 1024
[SwitchA-vlan1024] port gigabitethernet 1/0/1
```

**# Enable IGMP snooping for VLAN 1024.**

```
[SwitchA-vlan1024] igmp-snooping enable
[SwitchA-vlan1024] quit
```

**# Create VLAN 2, and enable IGMP snooping for this VLAN.**

```
[SwitchA] vlan 2
[SwitchA-vlan2] igmp-snooping enable
[SwitchA-vlan2] quit
```

**# Configure VLAN 3 and VLAN 4 in the same way. (Details not shown.)**

**# Configure GigabitEthernet 1/0/2 as a hybrid port, and configure VLAN 2 as the PVID.**

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type hybrid
[SwitchA-GigabitEthernet1/0/2] port hybrid pvid vlan 2
```

**# Assign GigabitEthernet 1/0/2 to VLAN 2 and VLAN 1024 as an untagged VLAN member.**

```
[SwitchA-GigabitEthernet1/0/2] port hybrid vlan 2 1024 untagged
[SwitchA-GigabitEthernet1/0/2] quit
```

**# Configure GigabitEthernet 1/0/3 as a hybrid port, and configure VLAN 3 as the PVID.**

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type hybrid
[SwitchA-GigabitEthernet1/0/3] port hybrid pvid vlan 3
```

**# Assign GigabitEthernet 1/0/3 to VLAN 3 and VLAN 1024 as an untagged VLAN member.**

```
[SwitchA-GigabitEthernet1/0/3] port hybrid vlan 3 1024 untagged
[SwitchA-GigabitEthernet1/0/3] quit
```

```

Configure GigabitEthernet 1/0/4 as a hybrid port, and configure VLAN 4 as the PVID.
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-type hybrid
[SwitchA-GigabitEthernet1/0/4] port hybrid pvid vlan 4

Assign GigabitEthernet 1/0/4 to VLAN 4 and VLAN 1024 as an untagged VLAN member.
[SwitchA-GigabitEthernet1/0/4] port hybrid vlan 4 1024 untagged
[SwitchA-GigabitEthernet1/0/4] quit

Configure VLAN 1024 as the multicast VLAN.
[SwitchA] multicast-vlan 1024

Assign GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 to VLAN 1024.
[SwitchA-mvlan-1024] port gigabitethernet 1/0/2 to gigabitethernet 1/0/4
[SwitchA-mvlan-1024] quit

```

## Verifying the configuration

1. Send IGMP reports from the receiver hosts in the user VLANs to join the multicast group **224.1.1.1**. (Details not shown.)
2. Verify that Switch A can receive the reports and that it can forward the reports to Router A.

# Display information about the multicast VLAN on Switch A.

```

[SwitchA] display multicast-vlan
Total 1 multicast-vlan(s)

```

```

Multicast vlan 1024

```

```

 subvlan list:
 no subvlan

```

```

 port list:

```

```

 GE1/0/2 GE1/0/3 GE1/0/4

```

# Display IGMP snooping group information on Switch A.

```

[SwitchA] display igmp-snooping group
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

```

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port

Subvlan flags: R-Real VLAN, C-Copy VLAN

```

Vlan(id):1024.

```

```

 Total 1 IP Group(s).
 Total 1 IP Source(s).
 Total 1 MAC Group(s).

```

```

 Router port(s):total 1 port.

```

```

 GE1/0/1 (D)

```

IP group(s):the following ip group(s) match to one mac group.

```

 IP group address:224.1.1.1
 (0.0.0.0, 224.1.1.1):

```



```

Host port(s):total 3 port.
 GE1/0/2 (D)
 GE1/0/3 (D)
 GE1/0/4 (D)
MAC group(s):
 MAC group address:0100-5e01-0101
 Host port(s):total 3 port.
 GE1/0/2
 GE1/0/3
 GE1/0/4

```

The output shows that IGMP snooping in the multicast VLAN (VLAN 1024) maintains the router port and the member ports.

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```

#
igmp-snooping
#
vlan 2
 igmp-snooping enable
#
vlan 3
 igmp-snooping enable
#
vlan 4
 igmp-snooping enable
#
vlan 1024
 igmp-snooping enable
#
multicast-vlan 1024
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 1024
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 to 2 1024 untagged
 port hybrid pvid vlan 2
 port multicast-vlan 1024
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type hybrid

```

```
port hybrid vlan 1 3 1024 untagged
port hybrid pvid vlan 3
port multicast-vlan 1024
#
interface GigabitEthernet1/0/4
port link-mode bridge
port link-type hybrid
port hybrid vlan 1 4 1024 untagged
port hybrid pvid vlan 4
port multicast-vlan 1024
#
```

# NQA configuration examples

This chapter provides NQA configuration examples.

## Example: Configuring an ICMP echo operation

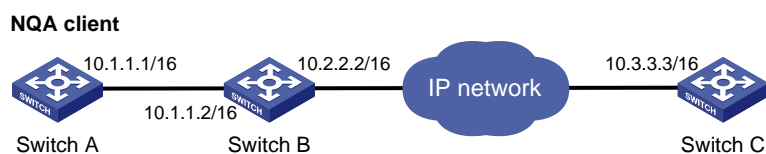
### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

### Network requirements

As shown in [Figure 131](#), 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 131 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 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 the operation finishes.

### Configuration procedures

# Create an ICMP echo operation and specify 10.3.3.3 as the destination IP address.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type icmp-echo
```

```

[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.3.3.3
Specify 10.1.1.2 as the next hop.
[SwitchA-nqa-admin-test-icmp-echo] next-hop 10.1.1.2
Configure the operation to repeat at an interval of 5000 milliseconds. If an operation is not completed
when the interval is reached, the next operation does not start. (By default, the time interval is 0
milliseconds, and only one operation is performed.)
[SwitchA-nqa-admin-test-icmp-echo] frequency 5000
Configure the ICMP echo operation to perform 10 probes.
[SwitchA-nqa-admin-test-icmp-echo] probe count 10
Enable saving history records and configure the maximum number of history records that can be saved
as 10.
[SwitchA-nqa-admin-test-icmp-echo] history-record enable
[SwitchA-nqa-admin-test-icmp-echo] history-record number 10
Start the ICMP echo operation.
[SwitchA-nqa-admin-test-icmp-echo] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever
After the ICMP echo operation runs for a period of time, stop the operation.
[SwitchA] undo nqa schedule admin test

```

## Verifying the configuration

```

Display the results of the ICMP echo operation.
[SwitchA] display nqa result admin test
 NQA entry(admin admin, tag test) test results:
 Destination IP address: 10.3.3.3
 Send operation times: 10 Receive response times: 10
 Min/Max/Average round trip time: 0/16/1
 Square-Sum of round trip time: 256
 Last succeeded probe time: 2012-08-23 15:00:01.2
 Extend results:
 Packet lost in test: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to sequence error: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
 Packet(s) arrived late: 0

```

# Display the history records of the ICMP echo operations.

```

[SwitchA] display nqa history admin test
 NQA entry(admin admin, tag test) history record(s):
 Index Response Status Time
 370 10 Succeeded 2012-08-23 15:00:01.2

```

|     |    |           |                       |
|-----|----|-----------|-----------------------|
| 369 | 10 | Succeeded | 2012-08-23 15:00:01.2 |
| 368 | 10 | Succeeded | 2012-08-23 15:00:01.2 |
| 367 | 10 | Succeeded | 2012-08-23 15:00:01.2 |
| 366 | 4  | Succeeded | 2012-08-23 15:00:01.2 |
| 365 | 10 | Succeeded | 2012-08-23 15:00:01.2 |
| 364 | 10 | Succeeded | 2012-08-23 15:00:01.1 |
| 363 | 10 | Succeeded | 2012-08-23 15:00:01.1 |
| 362 | 10 | Succeeded | 2012-08-23 15:00:01.1 |
| 361 | 4  | Succeeded | 2012-08-23 15:00:01.1 |

## Configuration files

```
#
nqa entry admin test
 type icmp-echo
 destination ip 10.3.3.3
 frequency 5000
 history-record enable
 history-record number 10
 next-hop 10.1.1.2
 probe count 10
#
nqa schedule admin test start-time now lifetime forever
#
```

## Example: Configuring a DHCP operation

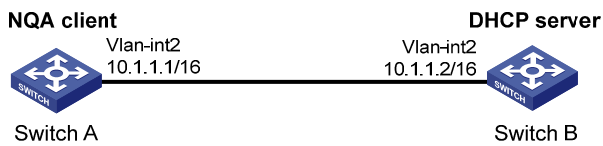
### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in [Figure 132](#), configure and schedule a DHCP operation to test the time for Switch A to obtain an IP address from the DHCP server Switch B.

**Figure 132 Network diagram**



## Configurations restrictions and guidelines

When you configure a DHCP operation, follow these restrictions and guidelines:

- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or the operation finishes.
- The DHCP operation requires a DHCP server. It also requires a DHCP relay agent if the client and server are on different subnets. Configure the DHCP server before the operation starts.

## Configuration procedures

# Create a DHCP operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type dhcp
```

# Specify VLAN-interface 2 as the operation interface.

```
[SwitchA-nqa-admin-test-dhcp] operation interface vlan-interface 2
```

# Enable the saving of history records.

```
[SwitchA-nqa-admin-test-dhcp] history-record enable
```

# Start the DHCP operation.

```
[SwitchA-nqa-admin-test-dhcp] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

# After the DHCP operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

## Verifying the configuration

# Display the results of the DHCP operation.

```
[SwitchA] display nqa result admin test
NQA entry(admin admin, tag test) test results:
 Send operation times: 1 Receive response times: 1
 Min/Max/Average round trip time: 624/624/624
 Square-Sum of round trip time: 389376
 Last succeeded probe time: 2012-11-22 09:56:03.2
Extend results:
```

```

Packet lost in test: 0%
Failures due to timeout: 0
Failures due to disconnect: 0
Failures due to no connection: 0
Failures due to sequence error: 0
Failures due to internal error: 0
Failures due to other errors: 0

Display the history records of the DHCP operation.
[SwitchA] display nqa history admin test
NQA entry(admin admin, tag test) history record(s):
 Index Response Status Time
 1 624 Succeeded 2012-11-22 09:56:03.2

```

## Configuration files

```

#
nqa entry admin test
 type dhcp
 history-record enable
 operation interface Vlan-interface2
#
nqa schedule admin test start-time now lifetime forever
#

```

## Example: Configuring a DNS operation

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in [Figure 133](#):

- Configure a DNS operation to test whether Switch A can translate the domain name **host.com** into an IP address through the DNS server.
- Test the time required for the resolution.

Figure 133 Network diagram



## Configurations restrictions and guidelines

When you configure a DNS operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you configure a DNS operation.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or the operation finishes.

## Configuration procedures

# Configure a DNS operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type dns
```

# Specify the IP address of the DNS server 10.2.2.2 as the destination address, and specify the domain name to be translated as **host.com**.

```
[SwitchA-nqa-admin-test-dns] destination ip 10.2.2.2
[SwitchA-nqa-admin-test-dns] resolve-target host.com
```

# Enable the saving of history records.

```
[SwitchA-nqa-admin-test-dns] history-record enable
```

# Start the DNS operation.

```
[SwitchA-nqa-admin-test-dns] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

# After the DNS operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

## Verifying the configuration

# Display the results of the DNS operation.

```
[SwitchA] display nqa result admin test
NQA entry(admin admin, tag test) test results:
 Destination IP address: 10.2.2.2
 Send operation times: 1 Receive response times: 1
 Min/Max/Average round trip time: 62/62/62
 Square-Sum of round trip time: 3844
```



```

 Last succeeded probe time: 2012-11-10 10:49:37.3
Extended results:
 Packet lost in test: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to sequence error: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
 Packet(s) arrived late: 0

Display the history records of the DNS operation.
[SwitchA] display nqa history admin test
NQA entry(admin admin, tag test) history record(s):
 Index Response Status Time
 1 62 Succeeded 2012-11-10 10:49:37.3

```

## Configuration files

```

#
nqa entry admin test
 type dns
 destination ip 10.2.2.2
 history-record enable
 resolve-target host.com
#
nqa schedule admin test start-time now lifetime forever
#

```

## Example: Configuring an FTP operation

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in [Figure 134](#), configure an FTP operation to test the time for Switch A to upload a file to the FTP server Switch B.

- The login username is **admin**.
- The login password is **systemtest**.

- The file to be transferred to the FTP server is **config.txt**.

**Figure 134 Network diagram**



## Configurations restrictions and guidelines

When you configure an FTP operation, follow these restrictions and guidelines:

- Make sure the switches can reach each other before you configure an FTP operation.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or the operation finishes.
- When you perform the FTP **put** operation, the NQA client will create a new operation file named *file-name* of a fixed size on the FTP server. This file is not one of the files saved on the NQA client.
- Use a small file and specify a longer duration for the FTP operation. A large file might result in transfer failure because of timeout.

## Configuration procedures

# Create an FTP operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type ftp
```

# Specify the IP address of the FTP server 10.2.2.2 as the destination address and specify 10.1.1.1 as the source IP address.

```
[SwitchA-nqa-admin-test-ftp] destination ip 10.2.2.2
[SwitchA-nqa-admin-test-ftp] source ip 10.1.1.1
```

# Specify **put** as the FTP operation type.

```
[SwitchA-nqa-admin-test-ftp] operation put
```

# Specify **config.txt** as the name of a file to be transferred.

```
[SwitchA-nqa-admin-test-ftp] filename config.txt
```

# Specify the FTP login username and password.

```
[SwitchA-nqa-admin-test-ftp] username admin
[SwitchA-nqa-admin-test-ftp] password systemtest
```

# Enable the saving of history records.

```
[SwitchA-nqa-admin-test-ftp] history-record enable
```

# Start the FTP operation.

```
[SwitchA-nqa-admin-test-ftp] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever

After the FTP operation runs for a period of time, stop the operation.
[SwitchA] undo nqa schedule admin test
```

## Verifying the configuration

# Display the results of the FTP operation.

```
[SwitchA] display nqa result admin test
NQA entry(admin admin, tag test) test results:
 Destination IP address: 10.2.2.2
 Send operation times: 1 Receive response times: 1
 Min/Max/Average round trip time: 173/173/173
 Square-Sum of round trip time: 29929
 Last succeeded probe time: 2012-11-22 10:07:28.6
 Extend results:
 Packet lost in test: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to sequence error: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
```

# Display the history records of the FTP operation.

```
[SwitchA] display nqa history admin test
NQA entry(admin admin, tag test) history record(s):
 Index Response Status Time
 1 173 Succeeded 2012-11-22 10:07:28.6
```

## Configuration files

```
#
nqa entry admin test
 type ftp
 destination ip 10.2.2.2
 filename config.txt
 history-record enable
 operation put
 password systemtest
 source ip 10.1.1.1
 username admin
#
nqa schedule admin test start-time now lifetime forever
#
```

# Example: Configuring an HTTP operation

## Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in [Figure 135](#), configure an HTTP operation on the NQA client to test the amount of time it takes for the client to obtain data from the HTTP server.

**Figure 135 Network diagram**



## Configurations restrictions and guidelines

When you configure an HTTP operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you configure an HTTP operation.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or the operation finishes.

## Configuration procedures

# Create an HTTP operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type http
```

# Specify the IP address of the HTTP server 10.2.2.2 as the destination address, and specify **index.htm** as the URL of the HTTP server.

```
[SwitchA-nqa-admin-test-http] destination ip 10.2.2.2
[SwitchA-nqa-admin-test-http] url /index.htm
```

# Enable the saving of history records.

```
[SwitchA-nqa-admin-test-http] history-record enable
```

```

Start the HTTP operation.
[SwitchA-nqa-admin-test-http] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever

After the HTTP operation runs for a period of time, stop the operation.
[SwitchA] undo nqa schedule admin test

```

## Verifying the configuration

```

Display the results of the HTTP operation.
[SwitchA] display nqa result admin test
NQA entry(admin admin, tag test) test results:
 Destination IP address: 10.2.2.2
 Send operation times: 1 Receive response times: 1
 Min/Max/Average round trip time: 64/64/64
 Square-Sum of round trip time: 4096
 Last succeeded probe time: 2012-11-22 10:12:47.9
 Extend results:
 Packet lost in test: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to sequence error: 0
 Failures due to internal error: 0
 Failures due to other errors: 0

Display the history records of the HTTP operation.
[SwitchA] display nqa history admin test
NQA entry(admin admin, tag test) history record(s):

```

| Index | Response | Status    | Time                  |
|-------|----------|-----------|-----------------------|
| 1     | 64       | Succeeded | 2012-11-22 10:12:47.9 |

## Configuration files

```

#
nqa entry admin test
 type http
 destination ip 10.2.2.2
 history-record enable
 url /index.htm
#
nqa schedule admin test start-time now lifetime forever
#

```

# Example: Configuring a UDP jitter operation

## Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in Figure 136, configure a UDP jitter operation to test the jitter, delay, and round-trip time between Switch A and Switch B.

Figure 136 Network diagram



## Configurations restrictions and guidelines

When you configure a UDP jitter operation, follow these restrictions and guidelines:

- Make sure the switches can reach each other before you configure a UDP jitter operation.
- You must configure Switch B as the NQA server before you configure a UDP jitter operation.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or the operation finishes.

## Configuration procedures

### Configuring Switch B

# Enable the NQA server. Configure a listening service to listen to the IP address 10.2.2.2 and UDP port 9000.

```
<SwitchB> system-view
[SwitchB] nqa server enable
[SwitchB] nqa server udp-echo 10.2.2.2 9000
```

### Configuring Switch A

# Create a UDP jitter operation.

```

<SwitchA> system-view
[SwitchA] nga entry admin test
[SwitchA-nga-admin-test] type udp-jitter

Configure 10.2.2.2 as the destination IP address and port 9000 as the destination port.
[SwitchA-nga-admin-test-udp-jitter] destination ip 10.2.2.2
[SwitchA-nga-admin-test-udp-jitter] destination port 9000

Configure the operation to repeat at an interval of 1000 milliseconds.
[SwitchA-nga-admin-test-udp-jitter] frequency 1000
[SwitchA-nga-admin-test-udp-jitter] quit

Start the UDP jitter operation.
[SwitchA] nga schedule admin test start-time now lifetime forever

After the UDP jitter operation runs for a period of time, stop the operation.
[SwitchA] undo nga schedule admin test

```

## Verifying the configuration

```

Display the results of the UDP jitter operation.
[SwitchA] display nga result admin test
 NQA entry (admin admin, tag test) test results:
 Destination IP address: 10.2.2.2
 Send operation times: 10 Receive response times: 10
 Min/Max/Average round trip time: 15/32/17
 Square-Sum of round trip time: 3235
 Last succeeded probe time: 2012-05-29 13:56:17.6
 Extended results:
 Packet loss in test: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to sequence error: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
 Packet(s) arrived late: 0
 UDP-jitter results:
 RTT number: 10
 Min positive SD: 4 Min positive DS: 1
 Max positive SD: 21 Max positive DS: 28
 Positive SD number: 5 Positive DS number: 4
 Positive SD sum: 52 Positive DS sum: 38
 Positive SD average: 10 Positive DS average: 10
 Positive SD square sum: 754 Positive DS square sum: 460
 Min negative SD: 1 Min negative DS: 6
 Max negative SD: 13 Max negative DS: 22
 Negative SD number: 4 Negative DS number: 5
 Negative SD sum: 38 Negative DS sum: 52

```

|                                      |                             |
|--------------------------------------|-----------------------------|
| Negative SD average: 10              | Negative DS average: 10     |
| Negative SD square sum: 460          | Negative DS square sum: 754 |
| One way results:                     |                             |
| Max SD delay: 15                     | Max DS delay: 16            |
| Min SD delay: 7                      | Min DS delay: 7             |
| Number of SD delay: 10               | Number of DS delay: 10      |
| Sum of SD delay: 78                  | Sum of DS delay: 85         |
| Square sum of SD delay: 666          | Square sum of DS delay: 787 |
| SD lost packet(s): 0                 | DS lost packet(s): 0        |
| Lost packet(s) for unknown reason: 0 |                             |

# Display the UDP jitter operation statistics.

[SwitchA] display nqa statistics admin test

NQA entry (admin admin, tag test) test statistics:

NO. : 1  
Destination IP address: 10.2.2.2  
Start time: 2012-05-29 13:56:14.0  
Life time: 47 seconds  
Send operation times: 410                      Receive response times: 410  
Min/Max/Average round trip time: 1/93/19  
Square-Sum of round trip time: 206176

Extended results:

Packet loss in test: 0%  
Failures due to timeout: 0  
Failures due to disconnect: 0  
Failures due to no connection: 0  
Failures due to sequence error: 0  
Failures due to internal error: 0  
Failures due to other errors: 0  
Packet(s) arrived late: 0

UDP-jitter results:

|                               |                               |
|-------------------------------|-------------------------------|
| RTT number: 410               |                               |
| Min positive SD: 3            | Min positive DS: 1            |
| Max positive SD: 30           | Max positive DS: 79           |
| Positive SD number: 186       | Positive DS number: 158       |
| Positive SD sum: 2602         | Positive DS sum: 1928         |
| Positive SD average: 13       | Positive DS average: 12       |
| Positive SD square sum: 45304 | Positive DS square sum: 31682 |
| Min negative SD: 1            | Min negative DS: 1            |
| Max negative SD: 30           | Max negative DS: 78           |
| Negative SD number: 181       | Negative DS number: 209       |
| Negative SD sum: 181          | Negative DS sum: 209          |
| Negative SD average: 13       | Negative DS average: 14       |
| Negative SD square sum: 46994 | Negative DS square sum: 3030  |

One way results:

|                         |                         |
|-------------------------|-------------------------|
| Max SD delay: 46        | Max DS delay: 46        |
| Min SD delay: 7         | Min DS delay: 7         |
| Number of SD delay: 410 | Number of DS delay: 410 |
| Sum of SD delay: 3705   | Sum of DS delay: 3891   |



```
Square sum of SD delay: 45987 Square sum of DS delay: 49393
SD lost packet(s): 0 DS lost packet(s): 0
Lost packet(s) for unknown reason: 0
```

---

**NOTE:**

The **display nqa history** command does not show any output for UDP jitter operations. Use the **display nqa result** command or the **display nqa statistics** command to display the UDP jitter operation result or statistics.

---

## Configuration files

- Switch B:

```
#
nqa server enable
nqa server udp-echo 10.2.2.2 9000
```
- Switch A:

```
#
nqa entry admin test
type udp-jitter
destination ip 10.2.2.2
destination port 9000
frequency 1000
#
nqa schedule admin test start-time now lifetime forever
#
```

## Example: Configuring an SNMP operation

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in [Figure 137](#), configure an SNMP operation to test the time for the NQA client to get a response packet from the SNMP agent Switch B.

Figure 137 Network diagram



## Configurations restrictions and guidelines

When you configure an SNMP operation, follow these restrictions and guidelines:

- Make sure the switches can reach each other before you configure an SNMP operation.
- You must configure Switch B as the SNMP agent before you configure an SNMP operation.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or the operation finishes.

## Configuration procedures

### Configuring Switch B (SNMP agent)

# Enable the SNMP agent, and set the SNMP version to **all**, the read community to **public**, and the write community to **private**.

```
<SwitchB> system-view
[SwitchB] snmp-agent
[SwitchB] snmp-agent sys-info version all
[SwitchB] snmp-agent community read public
[SwitchB] snmp-agent community write private
```

### Configuring Switch A

# Create an SNMP operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type snmp
```

# Configure the IP address of the SNMP agent 10.2.2.2 as the destination IP address.

```
[SwitchA-nqa-admin-test-snmp] destination ip 10.2.2.2
```

# Enable the saving of history records.

```
[SwitchA-nqa-admin-test-snmp] history-record enable
```

# Start the SNMP operation.

```
[SwitchA-nqa-admin-test-snmp] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

# After the SNMP operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

## Verifying the configuration

# Display the results of the SNMP operation.

```
[SwitchA] display nqa result admin test
NQA entry(admin admin, tag test) test results:
 Destination IP address: 10.2.2.2
 Send operation times: 1 Receive response times: 1
 Min/Max/Average round trip time: 50/50/50
 Square-Sum of round trip time: 2500
 Last succeeded probe time: 2012-11-22 10:24:41.1
Extend results:
 Packet lost in test: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to sequence error: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
```

# Display the history records of the SNMP operation.

```
[SwitchA] display nqa history admin test
NQA entry(admin admin, tag test) history record(s):
 Index Response Status Time
 1 50 Timeout 2012-11-22 10:24:41.1
```

## Configuration files

- Switch B:

```
#
snmp-agent
snmp-agent local-engineid 800063A20300E0FC123456
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info version all
```
- Switch A:

```
#
nqa entry admin test
 type snmp
 destination ip 10.2.2.2
 history-record enable
#
nqa schedule admin test start-time now lifetime forever
#
```

# Example: Configuring a TCP operation

## Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in [Figure 138](#), configure a TCP operation to test the time for the NQA client Switch A to establish a TCP connection to the NQA server Switch B.

**Figure 138 Network diagram**



## Configurations restrictions and guidelines

When you configure a TCP operation, follow these restrictions and guidelines:

- Make sure the switches can reach each other before you configure a TCP operation.
- You must configure Switch B as the NQA server before you configure a TCP operation.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or the operation finishes.

## 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 TCP port 9000.

```
<SwitchB> system-view
[SwitchB] nqa server enable
[SwitchB] nqa server tcp-connect 10.2.2.2 9000
```

### Configuring Switch A

# Create a TCP operation.

```

<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type tcp

Specify 10.2.2.2 as the destination IP address and port 9000 as the destination port.
[SwitchA-nqa-admin-test-tcp] destination ip 10.2.2.2
[SwitchA-nqa-admin-test-tcp] destination port 9000

Enable the saving of history records.
[SwitchA-nqa-admin-test-tcp] history-record enable

Start the TCP operation.
[SwitchA-nqa-admin-test-tcp] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever

After the TCP operation runs for a period of time, stop the operation.
[SwitchA] undo nqa schedule admin test

```

## Verifying the configuration

```

Display the results of the TCP operation.
[SwitchA] display nqa result admin test
 NQA entry(admin admin, tag test) test results:
 Destination IP address: 10.2.2.2
 Send operation times: 1 Receive response times: 1
 Min/Max/Average round trip time: 13/13/13
 Square-Sum of round trip time: 169
 Last succeeded probe time: 2012-11-22 10:27:25.1
 Extend results:
 Packet lost in test: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to sequence error: 0
 Failures due to internal error: 0
 Failures due to other errors: 0

Display the history records of the TCP operation.
[SwitchA] display nqa history admin test
 NQA entry(admin admin, tag test) history record(s):
 Index Response Status Time
 --- -
 1 13 Succeeded 2012-11-22 10:27:25.1

```

## Configuration files

- Switch B:
 

```

#
nqa server enable
nqa server tcp-connect 10.2.2.2 9000

```

- Switch A:
 

```
#
nqa entry admin test
 type tcp
 destination ip 10.2.2.2
 destination port 9000
 history-record enable
#
nqa schedule admin test start-time now lifetime forever
#
```

## Example: Configuring a UDP echo operation

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

### Network requirements

As shown in [Figure 139](#), configure a UDP echo operation to test the round-trip time between Switch A and Switch B.

**Figure 139 Network diagram**



### Configurations restrictions and guidelines

When you configure a UDP echo operation, follow these restrictions and guidelines:

- Make sure the switches can reach each other before you configure a UDP operation.
- You must configure Switch B as the NQA server before you configure a UDP operation.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or the operation finishes.

# 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: 25/25/25
 Square-Sum of round trip time: 625
 Last succeeded probe time: 2012-11-22 10:36:17.9
Extend results:
 Packet lost in test: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to sequence error: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
```

```
Display the history records of the UDP echo operation.
```

```
[SwitchA] display nqa history admin test
```

```
NQA entry(admin admin, tag test) history record(s):
```

| Index | Response | Status    | Time                  |
|-------|----------|-----------|-----------------------|
| 1     | 25       | Succeeded | 2012-11-22 10:36:17.9 |

## Configuration files

- Switch B:

```

nqa server enable
nqa server udp-echo 10.2.2.2 8000
```

- Switch A:

```

nqa entry admin test
type udp-echo
destination ip 10.2.2.2
destination port 8000
history-record enable

nqa schedule admin test start-time now lifetime forever

#
```

## Example: Configuring a voice operation

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in [Figure 140](#), configure a voice operation to test jitters and voice quality for voice packets between Switch A and Switch B.

**Figure 140 Network diagram**





## Configurations restrictions and guidelines

When you configure a voice operation, follow these restrictions and guidelines:

- Make sure the switches can reach each other before you configure a voice operation.
- You must configure Switch B as the NQA server before you configure a voice operation.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or the operation finishes.

## Configuration procedures

### Configuring Switch B

# Enable the NQA server, and configure a listening service to listen to IP address 10.2.2.2 and UDP port 9000.

```
<SwitchB> system-view
[SwitchB] nqa server enable
[SwitchB] nqa server udp-echo 10.2.2.2 9000
```

### Configuring Switch A

# Create a voice operation.

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type voice
```

# Specify 10.2.2.2 as the destination IP address and port 9000 as the destination port.

```
[SwitchA-nqa-admin-test-voice] destination ip 10.2.2.2
[SwitchA-nqa-admin-test-voice] destination port 9000
[SwitchA-nqa-admin-test-voice] quit
```

# Start the voice operation.

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

# After the voice operation runs for a period of time, stop the operation.

```
[SwitchA] undo nqa schedule admin test
```

## Verifying the configuration

# Display the results of the voice operation.

```
[SwitchA] display nqa result admin test
NQA entry(admin admin, tag test) test results:
 Destination IP address: 10.2.2.2
 Send operation times: 1000 Receive response times: 1000
 Min/Max/Average round trip time: 31/1328/33
 Square-Sum of round trip time: 2844813
 Last succeeded probe time: 2012-06-13 09:49:31.1
```

Extended results:

Packet lost in test: 0%  
Failures due to timeout: 0  
Failures due to disconnect: 0  
Failures due to no connection: 0  
Failures due to sequence error: 0  
Failures due to internal error: 0  
Failures due to other errors: 0  
Packet(s) arrived late: 0

Voice results:

RTT number: 1000

|                               |                                 |
|-------------------------------|---------------------------------|
| Min positive SD: 1            | Min positive DS: 1              |
| Max positive SD: 204          | Max positive DS: 1297           |
| Positive SD number: 257       | Positive DS number: 259         |
| Positive SD sum: 759          | Positive DS sum: 1797           |
| Positive SD average: 2        | Positive DS average: 6          |
| Positive SD square sum: 54127 | Positive DS square sum: 1691967 |
| Min negative SD: 1            | Min negative DS: 1              |
| Max negative SD: 203          | Max negative DS: 1297           |
| Negative SD number: 255       | Negative DS number: 259         |
| Negative SD sum: 759          | Negative DS sum: 1796           |
| Negative SD average: 2        | Negative DS average: 6          |
| Negative SD square sum: 53655 | Negative DS square sum: 1691776 |

One way results:

|                                      |                                |
|--------------------------------------|--------------------------------|
| Max SD delay: 343                    | Max DS delay: 985              |
| Min SD delay: 343                    | Min DS delay: 985              |
| Number of SD delay: 1                | Number of DS delay: 1          |
| Sum of SD delay: 343                 | Sum of DS delay: 985           |
| Square sum of SD delay: 117649       | Square sum of DS delay: 970225 |
| SD lost packet(s): 0                 | DS lost packet(s): 0           |
| Lost packet(s) for unknown reason: 0 |                                |

Voice scores:

MOS value: 4.38                      ICPIF value: 0

# Display the statistics of the voice operation.

[SwitchA] display nqa statistics admin test

NQA entry(admin admin, tag test) test statistics:

NO. : 1

Destination IP address: 10.2.2.2

Start time: 2012-06-13 09:45:37.8

Life time: 331

Send operation times: 4000                      Receive response times: 4000

Min/Max/Average round trip time: 15/1328/32

Square-Sum of round trip time: 7160528

Extended results:

Packet lost in test: 0%  
Failures due to timeout: 0  
Failures due to disconnect: 0  
Failures due to no connection: 0

```

Failures due to sequence error: 0
Failures due to internal error: 0
Failures due to other errors: 0
Packet(s) arrived late: 0
Voice results:
RTT number: 4000
Min positive SD: 1 Min positive DS: 1
Max positive SD: 360 Max positive DS: 1297
Positive SD number: 1030 Positive DS number: 1024
Positive SD sum: 4363 Positive DS sum: 5423
Positive SD average: 4 Positive DS average: 5
Positive SD square sum: 497725 Positive DS square sum: 2254957
Min negative SD: 1 Min negative DS: 1
Max negative SD: 360 Max negative DS: 1297
Negative SD number: 1028 Negative DS number: 1022
Negative SD sum: 1028 Negative DS sum: 1022
Negative SD average: 4 Negative DS average: 5
Negative SD square sum: 495901 Negative DS square sum: 5419

One way results:
Max SD delay: 359 Max DS delay: 985
Min SD delay: 0 Min DS delay: 0
Number of SD delay: 4 Number of DS delay: 4
Sum of SD delay: 1390 Sum of DS delay: 1079
Square sum of SD delay: 483202 Square sum of DS delay: 973651
SD lost packet(s): 0 DS lost packet(s): 0
Lost packet(s) for unknown reason: 0

Voice scores:
Max MOS value: 4.38 Min MOS value: 4.38
Max ICPIF value: 0 Min ICPIF value: 0

```

---

**NOTE:**

The **display nqa history** command does not show any output for voice operations. Use the **display nqa result** command or the **display nqa statistics** command to display the voice operation result or statistics.

---

## Configuration files

- Switch B:

```

#
nqa server enable
nqa server udp-echo 10.2.2.2 8000

```
- Switch A:

```

#
nqa entry admin test
type voice
destination ip 10.2.2.2
destination port 9000

```

```
#
nqa schedule admin test start-time now lifetime forever
```

## Example: Configuring a DLSw operation

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

### Network requirements

As shown in [Figure 141](#), configure a DLSw operation to test the response time of the DLSw device.

**Figure 141 Network diagram**



### Configurations restrictions and guidelines

When you configure a DLSw operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you configure a DLSw operation.
- You can enter the operation type view or the operation view of an NQA operation only when the operation is not scheduled or the operation finishes.

### Configuration procedures

```
Create a DLSw operation.
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type dlsw

Specify 10.2.2.2 as the destination IP address.
[SwitchA-nqa-admin-test-dlsw] destination ip 10.2.2.2

Enable the saving of history records.
[SwitchA-nqa-admin-test-dlsw] history-record enable
```

```

Start the DLSw operation.
[SwitchA-nqa-admin-test-dlsw] quit
[SwitchA] nqa schedule admin test start-time now lifetime forever

After the DLSw operation runs for a period of time, stop the operation.
[SwitchA] undo nqa schedule admin test

```

## Verifying the configuration

```

Display the results of the DLSw operation.
[SwitchA] display nqa result admin test
 NQA entry(admin admin, tag test) test results:
 Destination IP address: 10.2.2.2
 Send operation times: 1 Receive response times: 1
 Min/Max/Average round trip time: 19/19/19
 Square-Sum of round trip time: 361
 Last succeeded probe time: 2012-11-22 10:40:27.7
 Extend results:
 Packet lost in test: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to sequence error: 0
 Failures due to internal error: 0
 Failures due to other errors: 0

Display the history records of the DLSw operation.
[SwitchA] display nqa history admin test
 NQA entry(admin admin, tag test) history record(s):

```

| Index | Response | Status    | Time                  |
|-------|----------|-----------|-----------------------|
| 1     | 19       | Succeeded | 2012-11-22 10:40:27.7 |

## Configuration files

```

#
nqa entry admin test
 type dlsw
 destination ip 10.2.2.2
 history-record enable
#
nqa schedule admin test start-time now lifetime forever
#

```

# NTP configuration examples

This chapter provides NTP configuration examples.

**Table 8 NTP association modes**

| Mode                     | Clock source                                                                                                                                                                                                                                                                                                             | Time accuracy | Principle                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client/server            | <ul style="list-style-type: none"> <li>A client synchronizes to a server.</li> <li>A client can synchronize to multiple time servers.</li> </ul>                                                                                                                                                                         | High          | <ul style="list-style-type: none"> <li>Configure only the client.</li> <li>A client and a server can be in the same subnet or in different subnets.</li> <li>A client can synchronize to a server, but a server cannot synchronize to a client.</li> <li>Specify the IP address for the server on each client when the IP address of the reference source changes.</li> <li>Applicable to a network environment when the reference source is stable.</li> </ul> |
| Symmetric active/passive | <ul style="list-style-type: none"> <li>A symmetric active peer and a symmetric passive peer can synchronize to each other. If both of them are synchronized, the peer with a higher stratum synchronizes to the peer with a lower stratum.</li> <li>An active peer can synchronize to multiple passive peers.</li> </ul> | High          | <ul style="list-style-type: none"> <li>Configure only the active peer.</li> <li>A symmetric active peer and a symmetric passive peer can be in the same subnet or in different subnets.</li> <li>A symmetric active peer and a symmetric passive peer can synchronize to each other.</li> </ul>                                                                                                                                                                 |
| Broadcast                | When a client receives the first broadcast message from a server, the client uses the server as the clock source if the stratum in the message is lower than the stratum of the client. The client also synchronizes its clock to the server. Otherwise, the client uses its own clock.                                  | Low           | <ul style="list-style-type: none"> <li>Configure both the client and server.</li> <li>A client and a server must be in the same subnet.</li> <li>Configure NTP only on the server if the IP address of the clock source changes.</li> <li>The broadcast mode is intended for configurations involving one or a few servers and a potentially large client population.</li> </ul>                                                                                |

| Mode      | Clock source                                                                                                                                                                                                                                                                            | Time accuracy | Principle                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Multicast | When a client receives the first multicast message from a server, the client uses the server as the clock source if the stratum in the message is lower than the stratum of the client. The client also synchronizes its clock to the server. Otherwise, the client uses its own clock. | Low           | <ul style="list-style-type: none"> <li>Configure both the client and server.</li> <li>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.</li> <li>Configure only the server when the reference source changes.</li> <li>The broadcast mode is intended for configurations involving one or a few servers and a potentially large client population.</li> </ul> |

## Example: Configuring the NTP client/server mode

### Applicable product matrix

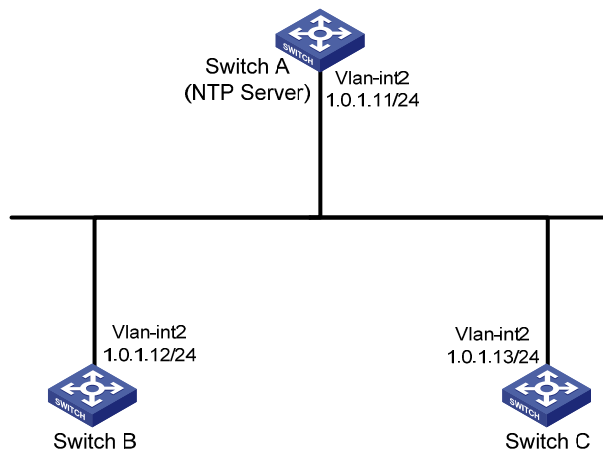
| Product series | Software version    |
|----------------|---------------------|
| HP 5500 EI     | Release series 2220 |
| HP 5500 SI     |                     |

### Network requirements

As shown in [Figure 142](#), 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 142 Network diagram**



## Configuration restrictions and guidelines

In this example, Switch A must be the device on which you can specify its local clock as the reference source.

## Configuration procedures

# Specify the local clock as the reference source, with the stratum level 2 on Switch A.

```
<SwitchA> system-view
[SwitchA] ntp-service refclock-master 2
```

# Specify Switch A as the NTP server of Switch B.

```
<SwitchB> system-view
[SwitchB] ntp-service unicast-server 1.0.1.11
```

# Specify Switch A as the NTP server of Switch C:

```
<SwitchC> system-view
[SwitchC] ntp-service unicast-server 1.0.1.11
```

## Verifying the configuration

# Display the NTP status of Switch B after clock synchronization.

```
[SwitchB] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 1.0.1.11
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 0.0000 ms
Root delay: 2.02 ms
Root dispersion: 1.05 ms
Peer dispersion: 7.81 ms
Reference time: 13:44:48.615 UTC Mar 23 2013(D4F83050.9D975F2C)
```

The output shows that Switch B has synchronized to Switch A. The clock stratum level is 3 on Switch B and 2 on Switch A.

# Display NTP association information for Switch B.

```
[SwitchB] display ntp-service sessions
 source reference stra reach poll now offset delay disper

[12345] 1.0.1.11 127.127.1.0 2 3 64 48 -1.3 2.3 0.5
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations : 1
```

The output shows that an association has been established between Switch B and Switch A.



## Configuration files

- Switch A:  
#  
ntp-service refclock-master 2
- Switch B:  
#  
ntp-service unicast-server 1.0.1.11
- Switch C:  
#  
ntp-service unicast-server 1.0.1.11

## Example: Configuring the NTP symmetric active/passive mode

### Applicable product matrix

| Product series | Software version    |
|----------------|---------------------|
| HP 5500 EI     | Release series 2220 |
| HP 5500 SI     |                     |

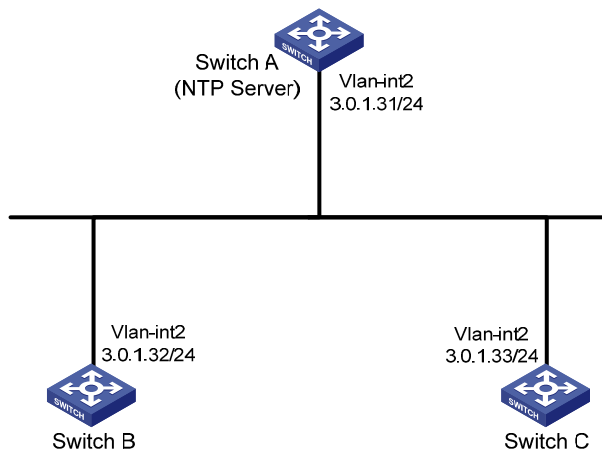
## Network requirements

As shown in [Figure 143](#), 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's local clock can be used as a reference source, so Switch C can synchronize to Switch B.

Figure 143 Network diagram



## Configuration restrictions and guidelines

In this example, make sure the local clocks of Switch A and Switch B can be configured as a reference source.

## Configuration procedures

# Specify the local clock as the reference source, with the stratum level 2 on Switch A.

```
<SwitchA> system-view
[SwitchA] ntp-service refclock-master 2
```

# Specify the local clock as the reference source, with the stratum level 3 on Switch B.

```
<SwitchB> system-view
[SwitchB] ntp-service refclock-master 3
```

# 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
Reference clock ID: 3.0.1.31
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: -0.2118 ms
Root delay: 2.68 ms
Root dispersion: 775.15 ms
Peer dispersion: 34.29 ms
Reference time: 14:08:20.264 UTC Mar 23 2013(D4F835D4.43AB862B)
```

The output shows that Switch B has synchronized to Switch A. The clock stratum level is 3 on Switch B and 2 on Switch A.

# Specify Switch A as the NTP server of Switch C.

```
<SwitchC> system-view
[SwitchC] ntp-service unicast-server 3.0.1.31
```

# Configure Switch B as a symmetric passive peer of Switch C.

```
[SwitchC] ntp-service unicast-peer 3.0.1.32
```

## Verifying the configuration

# Disconnect Switch A from the network. Display the NTP status of Switch C after clock synchronization.

```
[SwitchC] display ntp-service status
Clock status: synchronized
Clock stratum: 4
Reference clock ID: 3.0.1.32
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: -21.1982 ms
Root delay: 15.00 ms
Root dispersion: 775.15 ms
Peer dispersion: 34.29 ms
Reference time: 14:14:43.743 UTC Mar 23 2013(D4F83753.BE46F156)
```

The output shows that Switch C has synchronized to Switch B. The clock stratum level is 4 on Switch C and 3 on Switch B.

## Configuration files

- Switch A:

```
#
ntp-service refclock-master 2
```
- Switch B:

```
#
ntp-service refclock-master 3
ntp-service unicast-server 3.0.1.31
```
- Switch C:

```
#
ntp-service unicast-server 3.0.1.31
ntp-service unicast-peer 3.0.1.32
```

# Example: Configuring the NTP broadcast mode

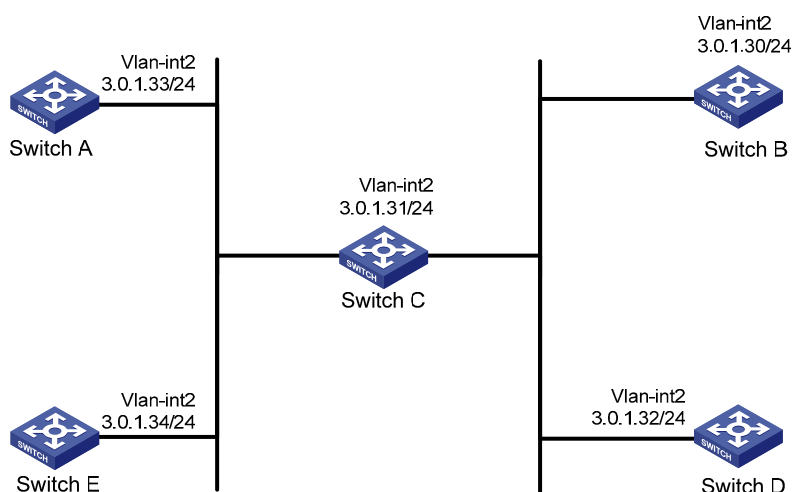
## Applicable product matrix

| Product series | Software version    |
|----------------|---------------------|
| HP 5500 EI     | Release series 2220 |
| HP 5500 SI     |                     |

## Network requirements

As shown in [Figure 144](#), configure NTP to synchronize the time among multiple devices on a subnet.

**Figure 144 Network diagram**



## Configuration restrictions and guidelines

In this example, Switch C must be the device on which you can specify its local clock as the reference source.

## Configuration procedures

# Specify the local clock as the reference source, with the stratum level 2 on Switch C.

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 2
```

# Configure Switch C to operate in broadcast server mode and send broadcast messages through VLAN-interface 2.

```
[SwitchC] interface Vlan-interface 2
```

```
[SwitchC-Vlan-interface2] ntp-service broadcast-server
```

# Configure Switch A to operate in broadcast client mode and receive broadcast messages on VLAN-interface 2.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 2
[SwitchA-Vlan-interface2] ntp-service broadcast-client
```

# Configure Switch B, Switch D, and Switch E in the same way Switch A is configured. (Details not shown.)

## Verifying the configuration

```
Display the NTP status of Switch A after clock synchronization.
[SwitchA-Vlan-interface2] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 0.0222 ms
Root delay: 2.28 ms
Root dispersion: 8.31 ms
Peer dispersion: 34.30 ms
Reference time: 14:14:43.743 UTC Mar 23 2013(D4F83753.BE46F156)
```

The output shows that Switch A has synchronized to Switch C. The clock stratum level is 3 on Switch A and 2 on Switch C.

```
Display NTP association information for Switch A.
[SwitchA-Vlan-interface2] display ntp-service sessions
 source reference stra reach poll now offset delay disper

[1234] 3.0.1.31 127.127.1.0 2 254 64 62 -16.0 32.0 16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations : 1
```

The output shows that an association has been set up between Switch A and Switch C.

## Configuration files

- Switch C:
 

```
#
ntp-service refclock-master 2
#
interface Vlan-interface2
ntp-service broadcast-server
```

- Switch A:  
#  
interface Vlan-interface2  
ntp-service broadcast-client
- Switch B:  
#  
interface Vlan-interface2  
ntp-service broadcast-client
- Switch D:  
#  
interface Vlan-interface2  
ntp-service broadcast-client
- Switch E:  
#  
interface Vlan-interface2  
ntp-service broadcast-client

## Example: Configuring the NTP multicast mode

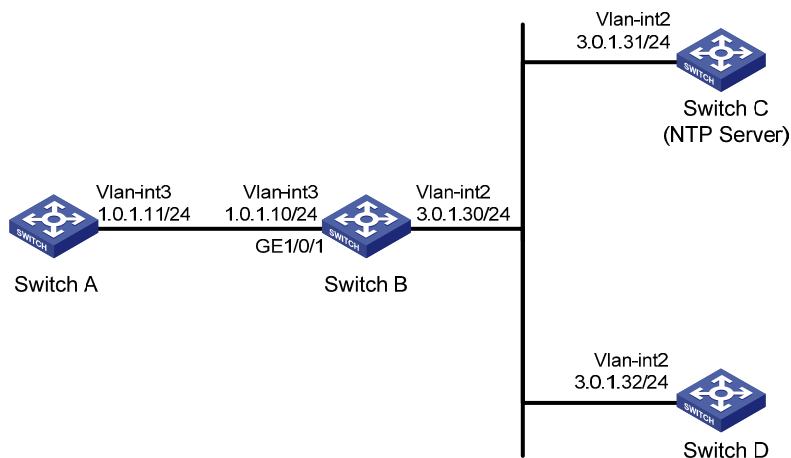
### Applicable product matrix

| Product series | Software version    |
|----------------|---------------------|
| HP 5500 EI     | Release series 2220 |
| HP 5500 SI     |                     |

### Network requirements

As shown in [Figure 145](#), configure NTP to synchronize the time among multiple devices on different subnets.

Figure 145 Network diagram



## Configuration restrictions and guidelines

When you configure NTP, follow these restrictions and guidelines:

- In this example, Switch B must support the multicast routing function.
- In this example, Switch C must be the device on which you can specify its local clock as the reference source.

## Configuration procedures

# Specify the local clock as the reference source, with the stratum level 2 on Switch C.

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 2
```

# Configure Switch C to operate in multicast server mode and send multicast messages through VLAN-interface 2.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service multicast-server
```

# Configure Switch D to operate in multicast client mode and receive multicast messages on VLAN-interface 2.

```
<SwitchD> system-view
[SwitchD] interface vlan-interface 2
[SwitchD-Vlan-interface2] ntp-service multicast-client
```

# Configure multicast functions on Switch B.

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] pim dm
[SwitchB-Vlan-interface2] quit
```

```
[SwitchB] vlan 3
[SwitchB-vlan3] port GigabitEthernet 1/0/1
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] igmp enable
[SwitchB-Vlan-interface3] igmp static-group 224.0.1.1
[SwitchB-Vlan-interface3] quit
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] igmp-snooping static-group 224.0.1.1 vlan 3
```

Switch A and Switch C are not on the same subnet, so you need to perform the following step. Otherwise, Switch A cannot receive multicast messages sent by Switch C.

# Configure Switch A to operate in multicast client mode and receive multicast messages on VLAN-interface 3.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ntp-service multicast-client
```

## Verifying the configuration

# Display the NTP status of Switch A after clock synchronization.

```
[SwitchA-Vlan-interface3] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 64.0000 Hz
Actual frequency: 64.0000 Hz
Clock precision: 2^7
Clock offset: 0.0000 ms
Root delay: 40.00 ms
Root dispersion: 10.83 ms
Peer dispersion: 34.30 ms
Reference time: 16:30:57.077 UTC Mar 23 2013(D4F85741.13F0AA21)
```

The output shows that Switch A has synchronized to Switch C. The clock stratum level is 3 on Switch A and 2 on Switch C.

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:
 

```
#
interface Vlan-interface3
ntp-service multicast-client
```



- Switch B:
 

```
#
multicast routing-enable
#
igmp-snooping
#
interface Vlan-interface2
pim dm
#
interface Vlan-interface3
igmp enable
igmp static-group 224.0.1.1
#
interface GigabitEthernet1/0/1
port link-mode bridge
port access vlan 3
igmp-snooping static-group 224.0.1.1 vlan 3
```
- Switch C:
 

```
#
ntp-service refclock-master 2
#
interface Vlan-interface2
ntp-service multicast-server
```
- Switch D:
 

```
#
interface Vlan-interface2
ntp-service multicast-client
```

## Example: Configuring the NTP broadcast mode with authentication

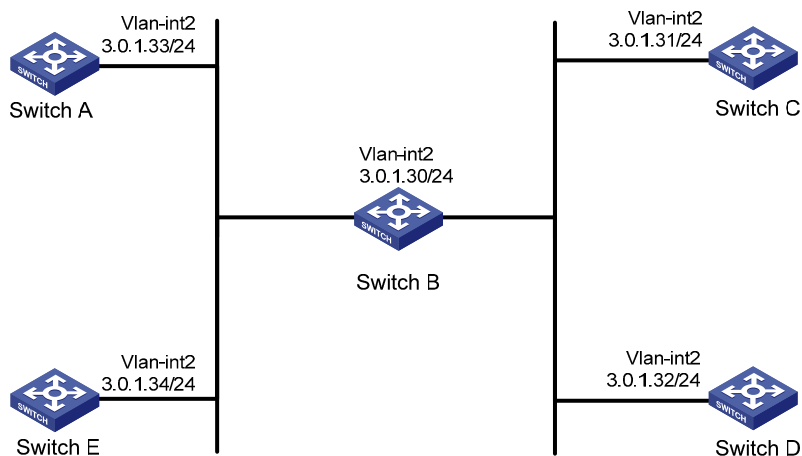
### Applicable product matrix

| Product series | Software version    |
|----------------|---------------------|
| HP 5500 EI     | Release series 2220 |
| HP 5500 SI     |                     |

### Network requirements

As shown in [Figure 146](#), configure NTP to synchronize the time among multiple devices on a subnet. Configure NTP authentication to prevent attacks.

Figure 146 Network diagram



## Configuration restrictions and guidelines

In this example, Switch C must be the device on which you can specify its local clock as the reference source.

## Configuration procedures

# Specify the local clock as the reference source, with the stratum level 2 on Switch C.

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 2
```

# 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 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
```

# 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> system-view
[SwitchA] ntp-service authentication enable
[SwitchA] ntp-service authentication-keyid 88 authentication-mode md5 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
```

# Configure Switch B, Switch D, and Switch E in the same way Switch A is configured. (Details not shown.)

## Verifying the configuration

# Display NTP service status on Switch A.

```
[SwitchA-Vlan-interface2] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 64.0000 Hz
Actual frequency: 64.0000 Hz
Clock precision: 2^7
Clock offset: 0.0000 ms
Root delay: 31.00 ms
Root dispersion: 8.31 ms
Peer dispersion: 34.30 ms
Reference time: 16:30:57.077 UTC Mar 23 2013(D4F85741.13F0AA21)
```

The output shows that Switch A has synchronized to Switch C. The clock stratum level is 3 on Switch A and 2 on Switch C.

## Configuration files

- Switch C:

```
#
interface Vlan-interface2
 ntp-service broadcast-server authentication-keyid 88
#
 ntp-service authentication enable
 ntp-service authentication-keyid 88 authentication-mode md5 cipher c3$xIhFrW3
Xg/dlKa9lUdCeCS5+2KGa/LrjDQ==
 ntp-service reliable authentication-keyid 88
 ntp-service refclock-master 3
#
```

- Switch A, Switch B, Switch D, and Switch E:

```
#
interface Vlan-interface2
 ntp-service broadcast-client
#
 ntp-service authentication enable
 ntp-service authentication-keyid 88 authentication-mode md5 cipher c3$1hqBL+J
I6q4WcVvPsXmC2pmvtYct5g
 ntp-service reliable authentication-keyid 88
#
```

# OSPF configuration examples

This chapter provides OSPF configuration examples.

## Example: Configuring basic OSPF

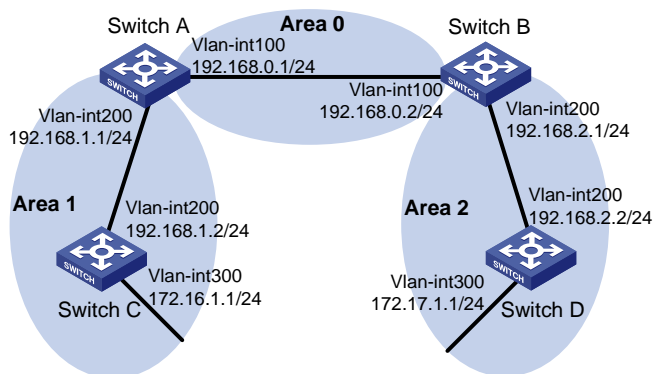
### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

### Network requirements

As shown in [Figure 147](#), configure OSPF on the switches and split the AS into three OSPF areas.

**Figure 147 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 147](#). (Details not shown.)
2. Enable OSPF:
  - # Configure Switch A.

```
<SwitchA> system-view
[SwitchA] router id 192.168.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

#### # Configure Switch B.

```
<SwitchB> system-view
[SwitchB] router id 192.168.2.1
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 2
[SwitchB-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.2] quit
[SwitchB-ospf-1] quit
```

#### # Configure Switch C.

```
<SwitchC> system-view
[SwitchC] router id 192.168.1.2
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

#### # Configure Switch D.

```
<SwitchD> system-view
[SwitchD] router id 192.168.2.2
[SwitchD] ospf
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
[SwitchD-ospf-1] quit
```

## Verifying the configuration

#### # Display information about OSPF neighbors on Switch A.

```
[SwitchA] display ospf peer verbose
```

```
OSPF Process 1 with Router ID 192.168.1.1
```

### Neighbors

```
Area 0.0.0.0 interface 192.168.0.1(Vlan-interface 100)'s neighbors
Router ID: 192.168.2.1 Address: 192.168.0.2 GR State: Normal
 State: Full Mode:Nbr is Master Priority: 1
 DR: 192.168.0.2 BDR: 192.168.0.1 MTU: 0
 Dead timer due in 36 sec
 Neighbor is up for 00:15:04
 Authentication Sequence: [0]
 Neighbor state change count: 3
```

### Neighbors

```
Area 0.0.0.1 interface 192.168.1.1(Vlan-interface 200)'s neighbors
Router ID: 192.168.1.2 Address: 192.168.1.2 GR State: Normal
 State: Full Mode:Nbr is Slave Priority: 1
 DR: 192.168.1.2 BDR: 192.168.1.1 MTU: 0
 Dead timer due in 39 sec
 Neighbor is up for 00:07:32
 Authentication Sequence: [0]
 Neighbor state change count: 2
```

The output shows that Switch A has established OSPF neighbor relationships with Switch B and Switch C.

# Display OSPF routing information on Switch A.

```
[SwitchA] display ospf routing
```

```
OSPF Process 1 with Router ID 192.168.1.1
 Routing Tables
```

```
Routing for Network
```

| Destination    | Cost | Type    | NextHop     | AdvRouter   | Area    |
|----------------|------|---------|-------------|-------------|---------|
| 172.16.1.0/24  | 1563 | Stub    | 192.168.1.2 | 172.16.1.1  | 0.0.0.1 |
| 172.17.1.0/24  | 3125 | Inter   | 192.168.0.2 | 192.168.2.1 | 0.0.0.0 |
| 192.168.1.0/24 | 1562 | Transit | 192.168.1.1 | 192.168.0.1 | 0.0.0.1 |
| 192.168.2.0/24 | 3124 | Inter   | 192.168.0.2 | 192.168.2.1 | 0.0.0.0 |
| 192.168.0.0/24 | 1562 | Transit | 192.168.0.1 | 192.168.0.1 | 0.0.0.0 |

```
Total Nets: 5
```

```
Intra Area: 3 Inter Area: 2 ASE: 0 NSSA: 0
```

# Display OSPF routing information on Switch D.

```
[SwitchD] display ospf routing
```

```
OSPF Process 1 with Router ID 192.168.2.2
 Routing Tables
```

```
Routing for Network
```

| Destination   | Cost | Type  | NextHop     | AdvRouter   | Area    |
|---------------|------|-------|-------------|-------------|---------|
| 172.16.1.0/24 | 4687 | Inter | 192.168.2.1 | 192.168.2.1 | 0.0.0.2 |
| 172.17.1.0/24 | 1    | Stub  | 172.17.1.1  | 192.168.2.2 | 0.0.0.2 |

```

192.168.1.0/24 4686 Inter 192.168.2.1 192.168.2.1 0.0.0.2
192.168.2.0/24 1562 Transit 192.168.2.2 192.168.2.2 0.0.0.2
192.168.0.0/24 3124 Inter 192.168.2.1 192.168.2.1 0.0.0.2

```

Total Nets: 5

Intra Area: 2 Inter Area: 3 ASE: 0 NSSA: 0

# On Switch D, ping the IP address 172.16.1.1 to test reachability.

```
[SwitchD] ping 172.16.1.1
```

```
 PING 172.16.1.1: 56 data bytes, press CTRL_C to break
```

```
 Reply from 172.16.1.1: bytes=56 Sequence=1 ttl=253 time=62 ms
```

```
 Reply from 172.16.1.1: bytes=56 Sequence=2 ttl=253 time=16 ms
```

```
 Reply from 172.16.1.1: bytes=56 Sequence=3 ttl=253 time=62 ms
```

```
 Reply from 172.16.1.1: bytes=56 Sequence=4 ttl=253 time=94 ms
```

```
 Reply from 172.16.1.1: bytes=56 Sequence=5 ttl=253 time=63 ms
```

```
--- 172.16.1.1 ping statistics ---
```

```
 5 packet(s) transmitted
```

```
 5 packet(s) received
```

```
 0.00% packet loss
```

```
 round-trip min/avg/max = 16/59/94 ms
```

The output shows that the destination is reachable.

## Configuration files

- Switch A:

```

#
router id 192.168.1.1
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 192.168.0.0 0.0.0.255
 area 0.0.0.1
 network 192.168.1.0 0.0.0.255
#

```

- Switch B:

```
#
```

```
router id 192.168.2.1
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.0.2 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 192.168.0.0 0.0.0.255
 area 0.0.0.2
 network 192.168.2.0 0.0.0.255
#
```

- Switch C:

```
#
router id 192.168.1.2
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 172.16.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.1
 network 192.168.1.0 0.0.0.255
 network 172.16.1.0 0.0.0.255
#
```

- Switch D:

```
#
router id 192.168.2.2
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ip address 192.168.2.2 255.255.255.0
#
```



```

interface Vlan-interface300
 ip address 172.17.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.2
 network 192.168.2.0 0.0.0.255
 network 172.17.1.0 0.0.0.255
#

```

## Example: Configuring an OSPF stub area

### Applicable product matrix

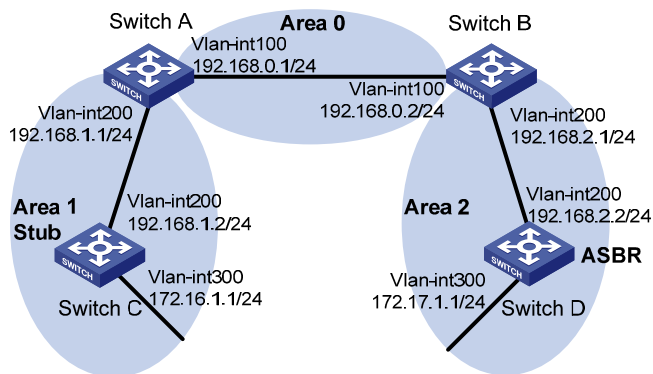
| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

### Network requirements

As shown in [Figure 148](#):

- Switch D acts as the ASBR to redistribute external routes.
- Run OSPF on the switches so that they can reach each other at the network layer.
- Configure Area 1 as a stub area to reduce the routing table size and LSAs.
- To further reduce the routing table size and advertised LSAs, configure the stub area as a totally stub area, which does not import inter-area routes or external routes.

**Figure 148 Network diagram**



# Configuration restrictions and guidelines

When you configure an OSPF stub area, follow these restrictions and guidelines:

- To configure a stub area, configure the **stub** command on all the switches attached to the area.
- To configure a totally stub area, configure the **stub** command on all the switches attached to the area and configure the **stub no-summary** command on the ABR.

## Configuration procedures

1. Configure IP addresses for the interfaces, as shown in [Figure 148](#). (Details not shown.)
2. Enable OSPF (see "[Example: Configuring basic OSPF](#)").
3. Configure route redistribution:

```
Configure Switch D to redistribute static routes.
```

```
[SwitchD] ip route-static 200.0.0.0 8 null 0
[SwitchD] ospf
[SwitchD-ospf-1] import-route static
[SwitchD-ospf-1] quit
```

```
Display OSPF routing information on Switch C.
```

```
[SwitchC] display ospf routing
 OSPF Process 1 with Router ID 192.168.1.2
 Routing Tables
```

```
Routing for Network
```

| Destination    | Cost | Type    | NextHop     | AdvRouter   | Area    |
|----------------|------|---------|-------------|-------------|---------|
| 172.16.1.0/24  | 1    | Stub    | 172.16.1.1  | 172.16.1.1  | 0.0.0.1 |
| 172.17.1.0/24  | 4687 | Inter   | 192.168.1.1 | 192.168.0.1 | 0.0.0.1 |
| 192.168.1.0/24 | 1562 | Transit | 192.168.1.2 | 172.16.1.1  | 0.0.0.1 |
| 192.168.2.0/24 | 4686 | Inter   | 192.168.1.1 | 192.168.0.1 | 0.0.0.1 |
| 192.168.0.0/24 | 3124 | Inter   | 192.168.1.1 | 192.168.0.1 | 0.0.0.1 |

```
Routing for ASEs
```

| Destination | Cost | Type  | Tag | NextHop     | AdvRouter  |
|-------------|------|-------|-----|-------------|------------|
| 200.0.0.0/8 | 10   | Type2 | 1   | 192.168.1.1 | 172.17.1.1 |

```
Total Nets: 6
```

```
Intra Area: 2 Inter Area: 3 ASE: 1 NSSA: 0
```

The output shows that Switch C's routing table contains an AS external route when Switch C resides in a normal OSPF area.

4. Configure Area 1 as a stub area:

```
Configure Switch A.
```

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
```

```

[SwitchA-ospf-1-area-0.0.0.1] stub
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
Configure Switch C.
[SwitchC] ospf
[SwitchC-ospf-1] stub-router
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] stub
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit

```

## Verifying the configuration

# Display OSPF routing information on Switch C.

```

[SwitchC] display ospf routing
 OSPF Process 1 with Router ID 192.168.1.2
 Routing Tables

```

Routing for Network

| Destination    | Cost  | Type    | NextHop     | AdvRouter   | Area    |
|----------------|-------|---------|-------------|-------------|---------|
| 0.0.0.0/0      | 65536 | Inter   | 192.168.1.1 | 192.168.0.1 | 0.0.0.1 |
| 172.16.1.0/24  | 1     | Stub    | 172.16.1.1  | 172.16.1.1  | 0.0.0.1 |
| 172.17.1.0/24  | 68660 | Inter   | 192.168.1.1 | 192.168.0.1 | 0.0.0.1 |
| 192.168.1.0/24 | 1562  | Transit | 192.168.1.2 | 172.16.1.1  | 0.0.0.1 |
| 192.168.2.0/24 | 68659 | Inter   | 192.168.1.1 | 192.168.0.1 | 0.0.0.1 |
| 192.168.0.0/24 | 67097 | Inter   | 192.168.1.1 | 192.168.0.1 | 0.0.0.1 |

Total Nets: 6

Intra Area: 2 Inter Area: 4 ASE: 0 NSSA: 0

The output shows that a default route has replaced the AS external route after the area where Switch C resides is configured as a stub area.

# Configure the area as a totally stub area by filtering Type-3 LSAs out of the stub area.

```

[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] stub no-summary
[SwitchA-ospf-1-area-0.0.0.1] quit

```

# Display OSPF routing information on Switch C.

```

[SwitchC] display ospf routing
 OSPF Process 1 with Router ID 172.16.1.1
 Routing Tables

```

Routing for Network

| Destination   | Cost | Type  | NextHop     | AdvRouter   | Area    |
|---------------|------|-------|-------------|-------------|---------|
| 0.0.0.0/0     | 1563 | Inter | 192.168.1.1 | 192.168.0.1 | 0.0.0.1 |
| 172.16.1.0/24 | 1    | Stub  | 172.16.1.1  | 172.16.1.1  | 0.0.0.1 |

```
192.168.1.0/24 1562 Transit 192.168.1.2 172.16.1.1 0.0.0.1
```

```
Total Nets: 3
```

```
Intra Area: 2 Inter Area: 1 ASE: 0 NSSA: 0
```

The output shows that inter-area routes have been removed, and only one external route (a default route) exists.

## Configuration files

- Switch A:

```
#
router id 192.168.1.1
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface200
ip address 192.168.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 192.168.0.0 0.0.0.255
area 0.0.0.1
network 192.168.1.0 0.0.0.255
stub no-summary
#
```

- Switch B:

```
#
router id 192.168.2.1
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
ip address 192.168.0.2 255.255.255.0
#
interface Vlan-interface200
ip address 192.168.2.1 255.255.255.0
#
ospf 1
area 0.0.0.0
```

```
network 192.168.0.0 0.0.0.255
area 0.0.0.2
network 192.168.2.0 0.0.0.255
#
```

- Switch C:

```
#
router id 192.168.1.2
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface300
ip address 172.16.1.1 255.255.255.0
#
ospf 1
stub-router
area 0.0.0.1
network 192.168.1.0 0.0.0.255
network 172.16.1.0 0.0.0.255
stub
#
```

- Switch D:

```
#
router id 192.168.2.2
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
ip address 192.168.2.2 255.255.255.0
#
interface Vlan-interface300
ip address 172.17.1.1 255.255.255.0
#
ospf 1
area 0.0.0.2
network 192.168.2.0 0.0.0.255
network 172.17.1.0 0.0.0.255
import-route static
#
ip route-static 200.0.0.0 255.0.0.0 NULL0
#
```

# Example: Configuring an OSPF NSSA area

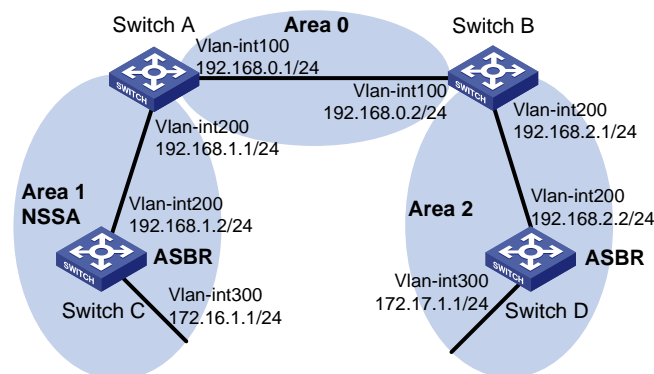
## Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

## Network requirements

As shown in [Figure 149](#), configure Area 1 as an NSSA area and configure Switch C to advertise redistributed external routes to other areas within the AS.

**Figure 149 Network diagram**



## Configuration restrictions and guidelines

When you configure an OSPF NSSA area, follow these restrictions and guidelines:

- To configure a stub area as an NSSA area, first remove the stub configuration by using the **undo stub** command.
- To configure an NSSA area, configure the **nssa** command on all the switches attached to the area.
- Virtual links cannot transit an NSSA area.

## Configuration procedures

1. Configure IP addresses for the interfaces, as shown in [Figure 149](#). (Details not shown.)
2. Enable OSPF (see "[Example: Configuring basic OSPF](#)").

3. Configure OSPF to redistribute static routes on Switch D (see "[Example: Configuring an OSPF stub area](#)").
4. Configure Area 1 as an NSSA area:

```
Configure Switch A.
```

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] nssa default-route-advertise no-summary
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

```
Configure Switch C.
```

```
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] nssa
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

---

**NOTE:**

- To allow Switch C in the NSSA area to reach other ASs, provide the keyword **default-route-advertise** for the **nssa** command configured on Switch A (the ABR) so that Switch C can obtain a default route.
  - Configuring the **nssa** command with the keyword **no-summary** on Switch A can reduce the routing table size on NSSA switches. On other NSSA switches, you only need to configure the **nssa** command.
- 

```
Display OSPF routing information on Switch C.
```

```
[SwitchC] display ospf routing
 OSPF Process 1 with Router ID 172.16.1.1
 Routing Tables
```

```
Routing for Network
```

| Destination    | Cost | Type  | NextHop     | AdvRouter   | Area    |
|----------------|------|-------|-------------|-------------|---------|
| 0.0.0.0/0      | 1563 | Inter | 192.168.1.1 | 192.168.0.1 | 0.0.0.1 |
| 172.16.1.0/24  | 1    | Stub  | 172.16.1.1  | 172.16.1.1  | 0.0.0.1 |
| 192.168.1.0/24 | 1562 | Stub  | 192.168.1.2 | 172.16.1.1  | 0.0.0.1 |

```
Total Nets: 3
```

```
Intra Area: 2 Inter Area: 1 ASE: 0 NSSA: 0
```

The output shows that the routing table of Switch C contains only a default route to reach other ASs.

```
Configure Switch C to redistribute a static route destined for network 100.0.0.0/8.
```

```
[SwitchC] ip route-static 100.0.0.0 8 null 0
[SwitchC] ospf
[SwitchC-ospf-1] import-route static
[SwitchC-ospf-1] quit
```

## Verifying the configuration

# Display OSPF routing information on Switch D.

```
[SwitchD-ospf-1] display ospf routing
 OSPF Process 1 with Router ID 172.17.1.1
 Routing Tables

Routing for Network
Destination Cost Type NextHop AdvRouter Area
172.16.1.0/24 4687 Inter 192.168.2.1 192.168.0.2 0.0.0.2
172.17.1.0/24 1 Transit 172.17.1.1 172.17.1.1 0.0.0.2
192.168.1.0/24 4686 Inter 192.168.2.1 192.168.0.2 0.0.0.2
192.168.2.0/24 1562 Transit 192.168.2.2 172.17.1.1 0.0.0.2
192.168.0.0/24 3124 Inter 192.168.2.1 192.168.0.2 0.0.0.2
Routing for ASEs
Destination Cost Type Tag NextHop AdvRouter
100.0.0.0/8 10 Type2 1 192.168.2.1 192.168.0.1

Routing for NSSAs
Destination Cost Type Tag NextHop AdvRouter

Total Nets: 6
Intra Area: 2 Inter Area: 3 ASE: 1 NSSA: 0
```

The output shows that the AS external route redistributed by the NSSA ASBR has been advertised to Area 2.

## Configuration files

- Switch A:

```
#
router id 192.168.1.1
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface200
ip address 192.168.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 192.168.0.0 0.0.0.255
```



```
area 0.0.0.1
 network 192.168.1.0 0.0.0.255
 nssa default-route-advertise no-summary
#
```

- **Switch B:**

```
#
 router id 192.168.2.1
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.0.2 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 192.168.0.0 0.0.0.255
 area 0.0.0.2
 network 192.168.2.0 0.0.0.255
#
```

- **Switch C:**

```
#
 router id 192.168.1.2
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 172.16.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.1
 network 192.168.1.0 0.0.0.255
 network 172.16.1.0 0.0.0.255
 nssa
 import-route static
#
 ip route-static 100.0.0.0 255.0.0.0 NULL0
#
```

- Switch D:

```
#
router id 192.168.2.2
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
ip address 192.168.2.2 255.255.255.0
#
interface Vlan-interface300
ip address 172.17.1.1 255.255.255.0
#
ospf 1
area 0.0.0.2
network 192.168.2.0 0.0.0.255
network 172.17.1.0 0.0.0.255
import-route static
#
ip route-static 200.0.0.0 255.0.0.0 NULL0
#
```

## Example: Configuring OSPF for a branch network

### Applicable product matrix

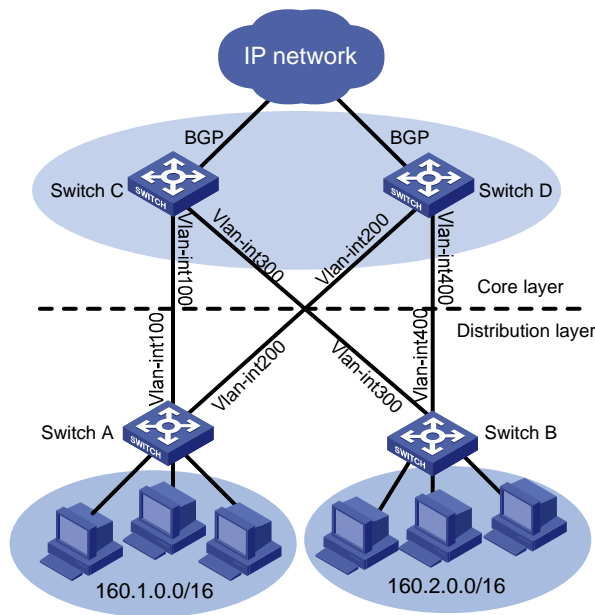
| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

### Network requirements

As shown in [Figure 150](#), the distribution switches, Switch A and Switch B, connect the branch networks. The core switches, Switch C and Switch D, connect the external IP network. Switch A and Switch B each provide dual uplinks to the two core switches for backup.

Configure the switches to make sure the branch networks and the external network can reach each other. To reduce the LSDB size, configure route summarization on Switch A and Switch B.

**Figure 150 Network diagram**



**Table 9 Interface and IP address assignment**

| Device   | Interface   | IP address  | Device   | Interface   | IP address  |
|----------|-------------|-------------|----------|-------------|-------------|
| Switch A | Vlan-int100 | 10.1.1.1/24 | Switch C | Vlan-int100 | 10.1.1.2/24 |
| Switch A | Vlan-int200 | 10.1.2.1/24 | Switch C | Vlan-int300 | 10.1.3.2/24 |
| Switch B | Vlan-int300 | 10.1.3.1/24 | Switch D | Vlan-int200 | 10.1.2.2/24 |
| Switch B | Vlan-int400 | 10.1.4.1/24 | Switch D | Vlan-int400 | 10.1.4.2/24 |

## Requirements analysis

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

- Configure the gateway of hosts in each branch network as the IP address of the switch's VLAN interface that connects to the hosts.
- Configure OSPF on Switch A, Switch B, Switch C, and Switch D.
- Configure OSPF to redistribute the branch networks on Switch A and Switch B so that Switch C and Switch D can learn the routes to the branch networks.
- Configure Switch C and Switch D to exchange routing information with the external network through BGP, and redistribute the learned routes into OSPF.

## Configuration procedures

This configuration example describes only OSPF-related configurations. For more information about BGP route learning and route redistribution, see *HP 5500 EI & 5500 SI Switch Series Layer 3—IP Routing Configuration Guide*.

1. Configure IP addresses for interfaces, as shown in [Figure 150](#). (Details not shown.)
2. Enable OSPF:

**# Configure Switch A.**

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

**# Configure Switch B.**

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
```

**# Configure Switch C.**

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

**# Configure Switch D.**

```
<SwitchD> system-view
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

**# Display routing information on Switch A. (Suppose Switch A connects three branch networks.)**

```
[SwitchA] display ip routing-table
```

```
Routing Tables: Public
```

```
Destinations : 14 Routes : 14
```

| Destination/Mask | Proto  | Pre | Cost | NextHop   | Interface |
|------------------|--------|-----|------|-----------|-----------|
| 10.1.1.0/24      | Direct | 0   | 0    | 10.1.1.1  | Vlan100   |
| 10.1.1.1/32      | Direct | 0   | 0    | 127.0.0.1 | InLoop0   |
| 10.1.2.0/24      | Direct | 0   | 0    | 10.1.2.1  | Vlan200   |
| 10.1.2.1/32      | Direct | 0   | 0    | 127.0.0.1 | InLoop0   |
| 10.1.3.0/24      | OSPF   | 10  | 2    | 10.1.1.2  | Vlan100   |
| 10.1.4.0/24      | OSPF   | 10  | 2    | 10.1.2.2  | Vlan200   |

|              |        |   |   |           |         |
|--------------|--------|---|---|-----------|---------|
| 127.0.0.0/8  | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |
| 127.0.0.1/32 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |
| 160.1.1.0/24 | Direct | 0 | 0 | 160.1.1.1 | Vlan1   |
| 160.1.1.1/32 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |
| 160.1.2.0/24 | Direct | 0 | 0 | 160.1.2.1 | Vlan2   |
| 160.1.2.1/32 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |
| 160.1.3.0/24 | Direct | 0 | 0 | 160.1.3.1 | Vlan3   |
| 160.1.3.1/32 | Direct | 0 | 0 | 127.0.0.1 | InLoop0 |

### 3. Configure route redistribution:

# Configure OSPF to redistribute direct routes on Switch A, and configure Switch A to advertise only summary route 160.1.0.0/16.

```
[SwitchA] ospf
[SwitchA-ospf-1] import-route direct
[SwitchA-ospf-1] asbr-summary 160.1.0.0 16
```

# Configure OSPF to redistribute direct routes on Switch B, and configure Switch B to advertise only summary route 160.2.0.0/16.

```
[SwitchB] ospf
[SwitchB-ospf-1] import-route direct
[SwitchB-ospf-1] asbr-summary 160.2.0.0 16
```

# Configure OSPF to redistribute routes from BGP on Switch C.

```
[SwitchC] ospf
[SwitchC-ospf-1] import-route bgp
```

# Configure OSPF to redistribute routes from BGP on Switch D.

```
[SwitchD] ospf
[SwitchD-ospf-1] import-route bgp
```

## Configuration files

- Switch A:

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.1 255.255.255.0
#
ospf 1
 asbr-summary 160.1.0.0 255.255.0.0
 import-route direct
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
```

```

 network 10.1.2.0 0.0.0.255
 #
 • Switch B:
 #
 vlan 300
 #
 vlan 400
 #
 interface Vlan-interface300
 ip address 10.1.3.1 255.255.255.0
 #
 interface Vlan-interface400
 ip address 10.1.4.1 255.255.255.0
 #
 ospf 1
 asbr-summary 160.2.0.0 255.255.0.0
 import-route direct
 area 0.0.0.0
 network 10.1.3.0 0.0.0.255
 network 10.1.4.0 0.0.0.255
 #
 • Switch C:
 #
 vlan 100
 #
 vlan 300
 #
 interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
 #
 interface Vlan-interface300
 ip address 10.1.3.2 255.255.255.0
 #
 ospf 1
 import-route bgp
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 10.1.3.0 0.0.0.255
 #
 • Switch D:
 #
 vlan 200
 #
 vlan 400
 #
 interface Vlan-interface200
 ip address 10.1.2.2 255.255.255.0

```

```
#
interface Vlan-interface400
 ip address 10.1.4.2 255.255.255.0
#
ospf 1
 import-route bgp
 area 0.0.0.0
 network 10.1.2.0 0.0.0.255
 network 10.1.4.0 0.0.0.255
#
```

## Example: Configuring OSPF to advertise a summary route

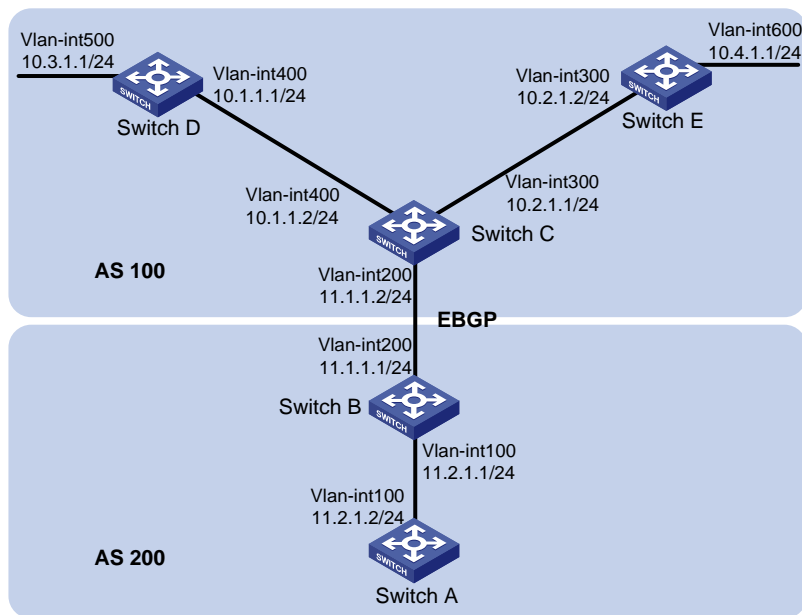
### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

### Network requirements

As shown in [Figure 151](#), AS 100 and AS 200 use BGP to exchange routing information. The switches in AS 100 and AS 200 run OSPF. Configure route summarization on Switch B to reduce the number of routes advertised to AS 200.

Figure 151 Network diagram



## Configuration restrictions and guidelines

When you configure OSPF to advertise a summary route, follow these restrictions and guidelines:

- Execute the **asbr-summary** command to enable an ASBR to do the following:
  - Summarize redistributed routes in the specified address range into a single route.
  - Advertise the summary route to neighbors.
- To enable the ASBR to advertise specific routes and not a summary route, execute the **undo asbr-summary** command.
- Only active OSPF routes that exist in the local OSPF routing table can be redistributed by BGP.

## Configuration procedures

1. Configure IP addresses for interfaces, as shown in Figure 151. (Details not shown.)
2. Enable OSPF:

# Configure Switch A.

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 11.2.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

# Configure Switch B.

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



```
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 11.2.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
```

#### # Configure Switch C.

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

#### # Configure Switch D.

```
<SwitchD> system-view
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
```

#### # Configure Switch E.

```
<SwitchE> system-view
[SwitchE] ospf
[SwitchE-ospf-1] area 0
[SwitchE-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchE-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
[SwitchE-ospf-1-area-0.0.0.0] quit
[SwitchE-ospf-1] quit
```

### 3. Configure an EBGP connection between Switch B and Switch C:

#### # Configure Switch B.

```
<SwitchB> system-view
[SwitchB] bgp 200
[SwitchB-bgp] peer 11.1.1.2 as-number 100
[SwitchB-bgp] quit
```

#### # Configure Switch C.

```
<SwitchC> system-view
[SwitchC] bgp 100
[SwitchC-bgp] peer 11.1.1.1 as-number 200
```

### 4. Configure route redistribution on Switch B and Switch C:

#### # Configure BGP to redistribute OSPF routes on Switch C.

```
[SwitchC-bgp] import-route ospf
```

#### # Configure BGP to redistribute direct routes on Switch C.

```
[SwitchC-bgp] import-route direct
```

#### # Configure OSPF to redistribute routes from BGP on Switch C.

```
[SwitchC] ospf
```

```
[SwitchC-ospf-1] import-route bgp
Configure BGP to redistribute OSPF routes on Switch B.
[SwitchB-bgp] import-route ospf
Configure BGP to redistribute direct routes on Switch B.
[SwitchB] bgp 200
[SwitchB-bgp] import-route direct
Configure OSPF to redistribute routes from BGP on Switch B.
[SwitchB] ospf
[SwitchB-ospf-1] import-route bgp
Display routing information on Switch A.
[SwitchA] display ip routing-table
Routing Tables: Public
 Destinations : 8 Routes : 8
```

| Destination/Mask | Proto  | Pre | Cost | NextHop   | Interface |
|------------------|--------|-----|------|-----------|-----------|
| 10.1.1.0/24      | O_ASE  | 150 | 1    | 11.2.1.1  | Vlan100   |
| 10.2.1.0/24      | O_ASE  | 150 | 1    | 11.2.1.1  | Vlan100   |
| 10.3.1.0/24      | O_ASE  | 150 | 1    | 11.2.1.1  | Vlan100   |
| 10.4.1.0/24      | O_ASE  | 150 | 1    | 11.2.1.1  | Vlan100   |
| 11.2.1.0/24      | Direct | 0   | 0    | 11.2.1.2  | Vlan100   |
| 11.2.1.2/32      | Direct | 0   | 0    | 127.0.0.1 | InLoop0   |
| 127.0.0.0/8      | Direct | 0   | 0    | 127.0.0.1 | InLoop0   |
| 127.0.0.1/32     | Direct | 0   | 0    | 127.0.0.1 | InLoop0   |

## 5. Configure route summarization on Switch B to advertise a summary route 10.0.0.0/8.

```
[SwitchB-ospf-1] asbr-summary 10.0.0.0 8
```

## Verifying the configuration

```
Display routing information on Switch A.
[SwitchA] display ip routing-table
Routing Tables: Public
 Destinations : 5 Routes : 5
```

| Destination/Mask | Proto  | Pre | Cost | NextHop   | Interface |
|------------------|--------|-----|------|-----------|-----------|
| 10.0.0.0/8       | O_ASE  | 150 | 2    | 11.2.1.1  | Vlan100   |
| 11.2.1.0/24      | Direct | 0   | 0    | 11.2.1.2  | Vlan100   |
| 11.2.1.2/32      | Direct | 0   | 0    | 127.0.0.1 | InLoop0   |
| 127.0.0.0/8      | Direct | 0   | 0    | 127.0.0.1 | InLoop0   |
| 127.0.0.1/32     | Direct | 0   | 0    | 127.0.0.1 | InLoop0   |

The output shows that routes 10.1.1.0/24, 10.2.1.0/24, 10.3.1.0/24, and 10.4.1.0/24 are summarized into a single route 10.0.0.0/8.

# Configuration files

- Switch A:

```
#
vlan 100
#
interface Vlan-interface100
 ip address 11.2.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 11.2.1.0 0.0.0.255
#
```

- Switch B:

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 11.2.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 11.1.1.1 255.255.255.0
#
bgp 200
 undo synchronization
 peer 11.1.1.2 as-number 100
 import-route direct
#
ospf 1
 asbr-summary 10.0.0.0 255.0.0.0
 import-route bgp
 area 0.0.0.0
 network 11.2.1.0 0.0.0.255
#
```

- Switch C:

```
#
vlan 200
#
vlan 300
#
vlan 400
#
interface Vlan-interface200
 ip address 11.1.1.2 255.255.255.0
```

```

#
interface Vlan-interface300
 ip address 10.2.1.1 255.255.255.0
#
interface Vlan-interface400
 ip address 10.1.1.2 255.255.255.0
#
bgp 100
 import-route ospf 1
 undo synchronization
 peer 11.1.1.1 as-number 200
 import-route direct
#
ospf 1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 10.2.1.0 0.0.0.255
 import-route bgp
#

```

- Switch D:

```

#
vlan 400
#
vlan 500
#
interface Vlan-interface400
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface500
 ip address 10.3.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 10.3.1.0 0.0.0.255
#

```

- Switch E:

```

#
vlan 300
#
vlan 600
#
interface Vlan-interface300
 ip address 10.2.1.2 255.255.255.0
#
interface Vlan-interface600
 ip address 10.4.1.1 255.255.255.0
#

```

```

ospf 1
 area 0.0.0.0
 network 10.2.1.0 0.0.0.255
 network 10.4.1.0 0.0.0.255
#

```

## Example: Configuring OSPF DR election

### Applicable product matrix

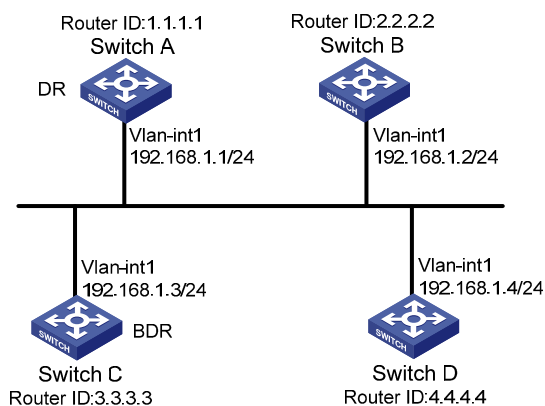
| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

### Network requirements

As shown in [Figure 152](#):

- Run OSPF on Switch A, Switch B, Switch C, and Switch D.
- Designate Switch A as the DR, and designate Switch C as the BDR.

**Figure 152 Network diagram**



### Configuration restrictions and guidelines

When you configure OSPF DR election, follow these restrictions and guidelines:

- If a switch with a higher router priority is added to the network after DR and BDR election, the switch cannot become the DR or BDR immediately because no DR election is performed for it. Therefore, the DR of a network might not be the switch with the highest priority, and the BDR might not be the switch with the second highest priority.

- The role of a switch is subnet (or interface) specific. It might be a DR on one interface and a BDR or DROther on another interface.

## Configuration procedures

1. Configure IP addresses for interfaces, as shown in [Figure 152](#). (Details not shown.)
2. Enable OSPF:

### # Configure Switch A.

```
<SwitchA> system-view
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

### # Configure Switch B.

```
<SwitchB> system-view
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

### # Configure Switch C.

```
<SwitchC> system-view
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

### # Configure Switch D.

```
<SwitchD> system-view
[SwitchD] router id 4.4.4.4
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

### # Display OSPF neighbor information on Switch A.

```
[SwitchA] display ospf peer verbose
```

```
OSPF Process 1 with Router ID 1.1.1.1
Neighbors
```

```

Area 0.0.0.0 interface 192.168.1.1(Vlan-interface1)'s neighbors
Router ID: 2.2.2.2 Address: 192.168.1.2 GR State: Normal
 State: 2-Way Mode: None Priority: 1
 DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
 Dead timer due in 38 sec
 Neighbor is up for 00:01:31
 Authentication Sequence: [0]
 Neighbor state change count: 2

Router ID: 3.3.3.3 Address: 192.168.1.3 GR State: Normal
 State: Full Mode: Nbr is Master Priority: 1
 DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
 Dead timer due in 31 sec
 Neighbor is up for 00:01:28
 Authentication Sequence: [0]
 Neighbor state change count: 2

Router ID: 4.4.4.4 Address: 192.168.1.4 GR State: Normal
 State: Full Mode: Nbr is Master Priority: 1
 DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
 Dead timer due in 31 sec
 Neighbor is up for 00:01:28
 Authentication Sequence: [0]
 Neighbor state change count: 2

```

The output shows that Switch D is the DR and Switch C is the BDR.

### 3. Configure router priorities on interfaces:

#### # Configure Switch A.

```

[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ospf dr-priority 3
[SwitchA-Vlan-interface1] quit

```

#### # Configure Switch C.

```

[SwitchC] interface vlan-interface 1
[SwitchC-Vlan-interface1] ospf dr-priority 2
[SwitchC-Vlan-interface] quit

```

#### # Configure Switch D.

```

[SwitchD] interface vlan-interface 1
[SwitchD-Vlan-interface1] ospf dr-priority 1
[SwitchD-Vlan-interface] quit

```

#### # Configure Switch B.

```

[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ospf dr-priority 0
[SwitchB-Vlan-interface1] quit

```

#### # Display neighbor information on Switch D.

```

[SwitchD] display ospf peer verbose

```

```

OSPF Process 1 with Router ID 4.4.4.4

```

## Neighbors

```
Area 0.0.0.0 interface 192.168.1.4(Vlan-interface1)'s neighbors
Router ID: 1.1.1.1 Address: 192.168.1.1 GR State: Normal
 State: Full Mode:Nbr is Slave Priority: 3
 DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
 Dead timer due in 31 sec
 Neighbor is up for 00:11:17
 Authentication Sequence: [0]
 Neighbor state change count: 3

Router ID: 2.2.2.2 Address: 192.168.1.2 GR State: Normal
 State: Full Mode:Nbr is Slave Priority: 0
 DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
 Dead timer due in 35 sec
 Neighbor is up for 00:11:19
 Authentication Sequence: [0]
 Neighbor state change count: 3

Router ID: 3.3.3.3 Address: 192.168.1.3 GR State: Normal
 State: Full Mode:Nbr is Slave Priority: 2
 DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
 Dead timer due in 33 sec
 Neighbor is up for 00:11:15
 Authentication Sequence: [0]
 Neighbor state change count: 3
```

The output shows that the DR and BDR are not changed, because the priority settings do not trigger a DR election.

## Verifying the configuration

# Restart the OSPF process of Switch D.

```
<SwitchD> reset ospf 1 process
Warning : Reset OSPF process? [Y/N]:y
```

# Display neighbor information on Switch D.

```
[SwitchD] display ospf peer verbose
```

```
OSPF Process 1 with Router ID 4.4.4.4
Neighbors
```

```
Area 0.0.0.0 interface 192.168.1.4(Vlan-interface1)'s neighbors
Router ID: 1.1.1.1 Address: 192.168.1.1 GR State: Normal
 State: Full Mode: Nbr is Slave Priority: 3
 DR: 192.168.1.3 BDR: 192.168.1.1 MTU: 0
 Dead timer due in 39 sec
 Neighbor is up for 00:01:40
```



```
Authentication Sequence: [0]
Neighbor state change count: 2
```

```
Router ID: 2.2.2.2 Address: 192.168.1.2 GR State: Normal
State: 2-Way Mode: None Priority: 0
DR: 192.168.1.3 BDR: 192.168.1.1 MTU: 0
Dead timer due in 35 sec
Neighbor is up for 00:01:44
Authentication Sequence: [0]
Neighbor state change count: 2
```

```
Router ID: 3.3.3.3 Address: 192.168.1.3 GR State: Normal
State: Full Mode: Nbr is Slave Priority: 2
DR: 192.168.1.3 BDR: 192.168.1.1 MTU: 0
Dead timer due in 39 sec
Neighbor is up for 00:01:41
Authentication Sequence: [0]
Neighbor state change count: 2
```

The output shows that Switch C becomes the DR, and Switch A becomes the BDR.

# Restart the OSPF process of Switch C.

```
<SwitchC> reset ospf 1 process
Warning : Reset OSPF process? [Y/N]:y
```

# Display neighbor information on Switch D.

```
[SwitchD] display ospf peer verbose
```

```
OSPF Process 1 with Router ID 4.4.4.4
Neighbors
```

```
Area 0.0.0.0 interface 192.168.1.4(Vlan-interfacel)'s neighbors
Router ID: 1.1.1.1 Address: 192.168.1.1 GR State: Normal
State: Full Mode: Nbr is Slave Priority: 3
DR: 192.168.1.1 BDR: 192.168.1.3 MTU: 0
Dead timer due in 39 sec
Neighbor is up for 00:01:40
Authentication Sequence: [0]
Neighbor state change count: 2
```

```
Router ID: 2.2.2.2 Address: 192.168.1.2 GR State: Normal
State: 2-Way Mode: None Priority: 0
DR: 192.168.1.1 BDR: 192.168.1.3 MTU: 0
Dead timer due in 35 sec
Neighbor is up for 00:01:44
Authentication Sequence: [0]
Neighbor state change count: 2
```

```
Router ID: 3.3.3.3 Address: 192.168.1.3 GR State: Normal
State: Full Mode: Nbr is Slave Priority: 2
```

```

DR: 192.168.1.1 BDR: 192.168.1.3 MTU: 0
Dead timer due in 39 sec
Neighbor is up for 00:01:41
Authentication Sequence: [0]
Neighbor state change count: 2

```

The output shows that Switch A becomes the DR, and Switch C becomes the BDR.

A neighbor state of **Full** indicates Switch D has established an adjacency with the neighbor. If the neighbor state is **2-way**, the two switches are not the DR or the BDR, and they do not exchange LSAs.

# Display OSPF interface information on Switch A.

```
[SwitchA] display ospf interface
```

```

OSPF Process 1 with Router ID 1.1.1.1
 Interfaces

Area: 0.0.0.0

```

| IP Address  | Type      | State | Cost | Pri | DR          | BDR         |
|-------------|-----------|-------|------|-----|-------------|-------------|
| 192.168.1.1 | Broadcast | DR    | 1    | 100 | 192.168.1.1 | 192.168.1.3 |

```
[SwitchB] display ospf interface
```

```

OSPF Process 1 with Router ID 2.2.2.2
 Interfaces

Area: 0.0.0.0

```

| IP Address  | Type      | State   | Cost | Pri | DR          | BDR         |
|-------------|-----------|---------|------|-----|-------------|-------------|
| 192.168.1.2 | Broadcast | DROther | 1    | 0   | 192.168.1.1 | 192.168.1.3 |

## Configuration files

- Switch A:

```

#
router id 1.1.1.1
#
interface Vlan-interface1
ip address 192.168.1.1 255.255.255.0
ospf dr-priority 3
#
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
#

```
- Switch B:

```

#
router id 2.2.2.2
#

```

```
interface Vlan-interface1
 ip address 192.168.1.2 255.255.255.0
 ospf dr-priority 0
#
ospf 1
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
#
```

- Switch C:

```
#
router id 3.3.3.3
#
interface Vlan-interface1
 ip address 192.168.1.3 255.255.255.0
 ospf dr-priority 2
#
ospf 1
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
#
```

- Switch D:

```
#
router id 4.4.4.4
#
interface Vlan-interface1
 ip address 192.168.1.4 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
#
```

## Example: Configuring an OSPF virtual link

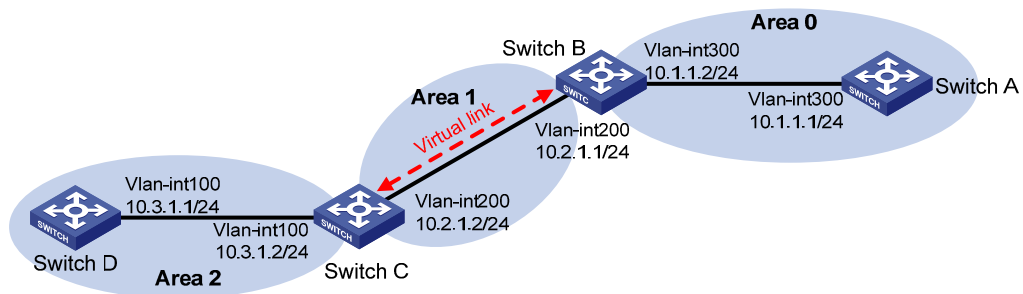
### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

## Network requirements

As shown in [Figure 153](#), Area 2 and Area 0 are not directly connected, and switches in Area 2 cannot reach switches in other areas. Configure a virtual link between Switch B and Switch C through Area 1 to connect the entire network so that all switches can reach each other.

**Figure 153 Network diagram**



## Configuration restrictions and guidelines

When you configure an OSPF virtual link, follow these restrictions and guidelines:

- Configure the **vlink-peer** command on both ends of a virtual link. The **hello** and **dead** intervals must be identical on both ends of the virtual link.
- Make sure you use the correct neighbor router ID when you configure a virtual link by using the **vlink-peer** command. The ID might or might not be the IP address of the neighbor interface.
- Virtual links cannot transit a stub area or an NSSA area.

## Configuration procedures

1. Configure IP addresses for interfaces, as shown in [Figure 153](#). (Details not shown.)
2. Enable OSPF:

# Configure Switch A.

```
<SwitchA> system-view
[SwitchA] ospf 1 router-id 1.1.1.1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
```

# Configure Switch B.

```
<SwitchB> system-view
[SwitchB] ospf 1 router-id 2.2.2.2
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
```

```
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.1] quit
```

### # Configure Switch C.

```
<SwitchC> system-view
[SwitchC] ospf 1 router-id 3.3.3.3
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] area 2
[SwitchC-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.2] quit
```

### # Configure Switch D.

```
<SwitchD> system-view
[SwitchD] ospf 1 router-id 4.4.4.4
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
```

### # Display OSPF routing information on Switch B.

```
[SwitchB] display ospf routing
 OSPF Process 1 with Router ID 2.2.2.2
 Routing Tables

Routing for Network
Destination Cost Type NextHop AdvRouter Area
10.2.1.0/24 2 Transit 10.2.1.1 3.3.3.3 0.0.0.1
10.1.1.0/24 2 Transit 10.1.1.2 2.2.2.2 0.0.0.0
Total Nets: 2
Intra Area: 2 Inter Area: 0 ASE: 0 NSSA: 0
```

The output shows that the routing table of Switch B has no route to Area 2 when Area 0 has no direct connection to Area 2.

## 3. Configure a virtual link:

### # Configure Switch B.

```
[SwitchB] ospf
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] vlink-peer 3.3.3.3
[SwitchB-ospf-1-area-0.0.0.1] quit
[SwitchB-ospf-1] quit
```

### # Configure Switch C.

```
[SwitchC] ospf 1
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[SwitchC-ospf-1-area-0.0.0.1] quit
```

## Verifying the configuration

# Display OSPF routing information on Switch B.

```
[SwitchB] display ospf routing
 OSPF Process 1 with Router ID 2.2.2.2
 Routing Tables
Routing for Network
Destination Cost Type NextHop AdvRouter Area
10.2.1.0/24 2 Transit 10.2.1.1 3.3.3.3 0.0.0.1
10.3.1.0/24 5 Inter 10.2.1.2 3.3.3.3 0.0.0.0
10.1.1.0/24 2 Transit 10.1.1.2 2.2.2.2 0.0.0.0
Total Nets: 3
Intra Area: 2 Inter Area: 1 ASE: 0 NSSA: 0
```

The output shows that Switch B has learned the route 10.3.1.0/24 to Area 2.

## Configuration files

- Switch A:

```
#
vlan 300
#
interface Vlan-interface300
 ip address 10.1.1.1 255.255.255.0
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
#
```
- Switch B:

```
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ip address 10.2.1.1 255.255.255.0
#
interface Vlan-interface300
 ip address 10.1.1.2 255.255.255.0
#
ospf 1 router-id 2.2.2.2
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 area 0.0.0.1
 network 10.2.1.0 0.0.0.255
```

- ```

    vlink-peer 3.3.3.3
#

```
- Switch C:

```

#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 10.3.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 10.2.1.2 255.255.255.0
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.1
  network 10.2.1.0 0.0.0.255
  vlink-peer 2.2.2.2
 area 0.0.0.2
  network 10.3.1.0 0.0.0.255
#

```
 - Switch D:

```

#
vlan 100
#
interface Vlan-interface100
 ip address 10.3.1.1 255.255.255.0
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.2
  network 10.3.1.0 0.0.0.255
#

```

Example: Configuring OSPF GR

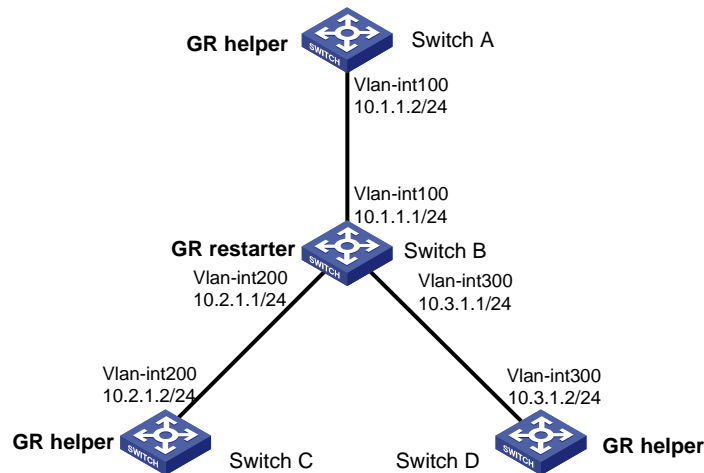
Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

Network requirements

As shown in [Figure 154](#), configure IETF Graceful Restart (GR) on Switch B. This avoids flapping, route changes, or forwarding interruption during an active/standby switchover or a routing protocol restart.

Figure 154 Network diagram



Configuration procedures

1. Configure IP addresses for interfaces, as shown in [Figure 154](#). (Details not shown.)
2. Enable OSPF:

Configure Switch A.

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

Configure Switch B.

```
<SwitchB> system-view
[SwitchB] ospf 1
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] return
```

Configure Switch C.

```
<SwitchC> system-view
[SwitchC] ospf 1
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
```



```
[SwitchC-ospf-1-area-0.0.0.0] return
# Configure Switch D.
<SwitchD> system-view
[SwitchD] ospf 1
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] return
```

3. Configure OSPF GR:

Configure Switch B as the IETF OSPF GR restarter.

```
<SwitchB> system-view
[SwitchB] ospf 1
[SwitchB-ospf-1] opaque-capability enable
[SwitchB-ospf-1] graceful-restart ietf
```

Configure Switch A as the GR helper.

```
<SwitchA> system-view
[SwitchA] ospf 1
[SwitchA-ospf-1] opaque-capability enable
```

Configure Switch C as the GR helper.

```
<SwitchC> system-view
[SwitchC] ospf 1
[SwitchC-ospf-1] opaque-capability enable
```

Configure Switch D as the GR helper.

```
<SwitchD> system-view
[SwitchD] ospf 1
[SwitchD-ospf-1] opaque-capability enable
```

Verifying the configuration

Restart the OSPF process on Switch B to trigger GR. During the GR process, verify that the routing tables of switches do not have any changes. Also verify that 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
 opaque-capability enable
 area 0.0.0.0
```

- ```

 network 10.1.1.0 0.0.0.255
#

```
- **Switch B:**

```

#
vlan 100
#
vlan 200
#
vlan 300
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 10.2.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 10.3.1.2 255.255.255.0
#
ospf 1
 opaque-capability enable
 graceful-restart ietf
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.2.1.0 0.0.0.255
 network 10.3.1.0 0.0.0.255
#

```
  - **Switch C:**

```

#
vlan 100
#
interface Vlan-interface100
 ip address 10.2.1.2 255.255.255.0
#
ospf 1
 opaque-capability enable
area 0.0.0.0
 network 10.2.1.0 0.0.0.255
#

```
  - **Switch D:**

```

#
vlan 300
#
interface Vlan-interface300
 ip address 10.3.1.2 255.255.255.0
#
ospf 1

```

```

opaque-capability enable
area 0.0.0.0
 network 10.3.1.0 0.0.0.255
#

```

## Example: Configuring BFD for OSPF

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

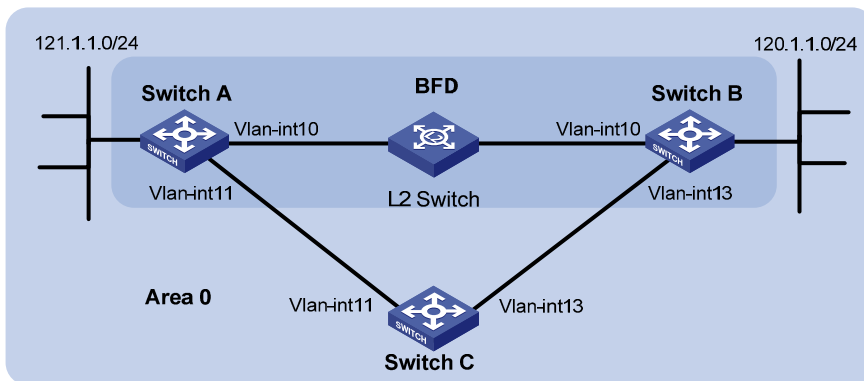
### Network requirements

As shown in [Figure 155](#):

- 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 155 Network diagram**



**Table 10 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 155](#). (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: QoSLeId:
 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: QoSLeId:
 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
#
```

# Patch installation examples

This document provides examples for fixing system bugs without rebooting the switch.

To fix system bugs, you can install patches in one step or step by step.

**Table 11 Patch installation methods**

| Method                          | Remarks                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Installing patches in one step  | Use a single command to install all patches.                                                                                                                                   |
| Installing patches step by step | Use a series of commands to specify the patches to be installed and install the specified patches.<br>You can track the status of the patches during the installation process. |

## General configuration restrictions and guidelines

When you install patches, follow these restrictions and guidelines:

- The version of the patches must match the version of the system software.
- The patch files must be named as specified in [Table 12](#). Otherwise, the system cannot find the files.

**Table 12 Default patch file names**

| Product series | Default patch file names |
|----------------|--------------------------|
| HP 5500 EI     | patch_xxx.bin            |
| HP 5500 SI     |                          |

## Example: Installing patches in one step

### Applicable product matrix

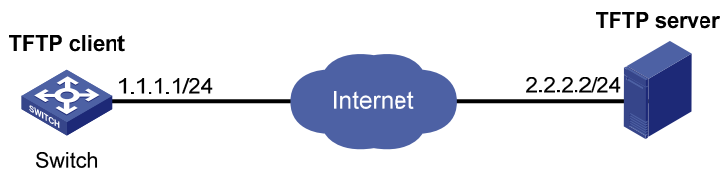
| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in [Figure 156](#), download the patches for the switch from the TFTP server and install the patches in one step.



Figure 156 Network diagram



## Configuration restrictions and guidelines

When you install patches in one step, follow these restrictions and guidelines:

- Make sure the switch has enough space to save the patch files.
- To use TFTP, set the file transfer mode to binary. Otherwise, the switch might not be able to resolve the patch files correctly.

## Configuration procedures

# Download the patch file **patch\_xxx.bin** from the TFTP server to the root directory of the switch's storage medium.

```
<Switch> tftp 2.2.2.2 get patch_xxx.bin
```

# Install the patches.

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

```
[Switch] patch install flash:
```

```
Patches will be installed. Continue? [Y/N]:y
```

```
Do you want to continue running patches after reboot? [Y/N]:y
```

```
Installing patches.....
```

```
Installation completed, and patches will continue to run after reboot.
```

## Verifying the configuration

# Display patch information. Verify that the patches are installed and running.

```
<Switch> display patch information
```

```
The location of patches: flash:
```

```
Slot Version Temporary Common Current Active Running Start-Address
```

```

1 XXX 0 0 0 0 0 0x53f8364
```

## Configuration files

The commands used for patch download and installation are not saved to the configuration file. They are one-time commands.

# Example: Installing patches step by step

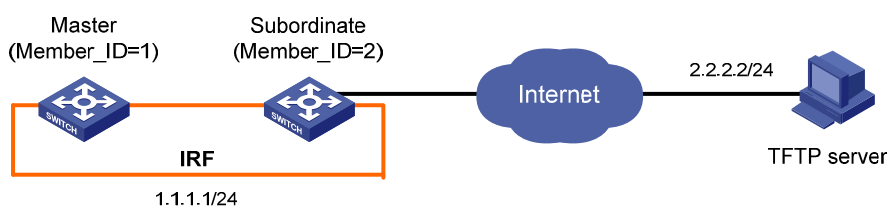
## Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in [Figure 157](#), download the patches for the switches from the TFTP server and install the patches step by step.

**Figure 157 Network diagram**



Note: The orange lines represent IRF links

## Configuration restrictions and guidelines

When you install patches step by step, follow these restrictions and guidelines:

- Make sure the switches have enough space to save the patch files.
- To use TFTP, set the file transfer mode to binary. Otherwise, the switch might not be able to resolve the patch files correctly.

## Configuration procedures

# Download the patch file **patch\_xxx.bin** from the TFTP server to the root directory of the master's storage medium.

```
<Switch> tftp 2.2.2.2 get patch_xxx.bin
```

# Download the patch file **patch\_xxx.bin** from the TFTP server to the root directory of the subordinate member's storage medium.

```
<Switch> tftp 2.2.2.2 get patch_xxx.bin slot2#flash:/patch_xxx.bin
```

# Set the patch file location to the root directory of the flash memory.

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

```

[Switch] patch location flash:

Load patches from the flash memory to the patch memory area on each member switch.
[Switch] patch load slot 1
[Switch] patch load slot 2

Activate patch 1 on the member switches.
[Switch] patch active 1 slot 1
[Switch] patch active 1 slot 2

Confirm the patch on the member switches.
[Switch] patch run 1 slot 1
[Switch] patch run 1 slot 2

```

## Verifying the configuration

```

Display patch information. Verify that the patches are installed and running.
<Switch> display patch information
The location of patches: flash:
Slot Version Temporary Common Current Active Running Start-Address

1 XXX 0 1 1 0 1 0x53f8364
2 XXX 0 1 1 0 1 0x53f8364

```

## Configuration files

The commands used for patch download and installation are not saved to the configuration file. They are one-time commands.

# PIM configuration examples

This chapter provides PIM configuration examples.

Based on the implementation mechanism, PIM includes the following categories:

- **Protocol Independent Multicast–Dense Mode**—PIM-DM uses the ASM model and is suitable for small-sized networks with densely distributed multicast members.
- **Protocol Independent Multicast–Sparse Mode**—PIM-SM uses the ASM model and is suitable for large- and medium-sized networks with sparsely and widely distributed multicast members. For refined management, PIM-SM employs the administrative scoping mechanism to provide services for private group addresses in specific admin-scoped zones.
- **Protocol Independent Multicast Source-Specific Multicast**—PIM-SSM provides a solution for source-specific multicast.

## General configuration restrictions and guidelines

When you configure PIM, follow these restrictions and guidelines:

- All the interfaces on a switch must operate in the same PIM mode.
- If a VLAN is running a Layer 2 multicast protocol, do not configure Layer 3 multicast protocols on the VLAN interface of this VLAN.

## Example: Configuring PIM-DM

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

### Network requirements

As shown in [Figure 158](#):

- All the switches are Layer 3 switches, and they run OSPF.
- The multicast source, receiver hosts, and switches can communicate with each other through unicast routes.

Configure PIM-DM on each switch, so that multicast data can be sent to receivers in **N1** and **N2**.

Figure 158 Network diagram

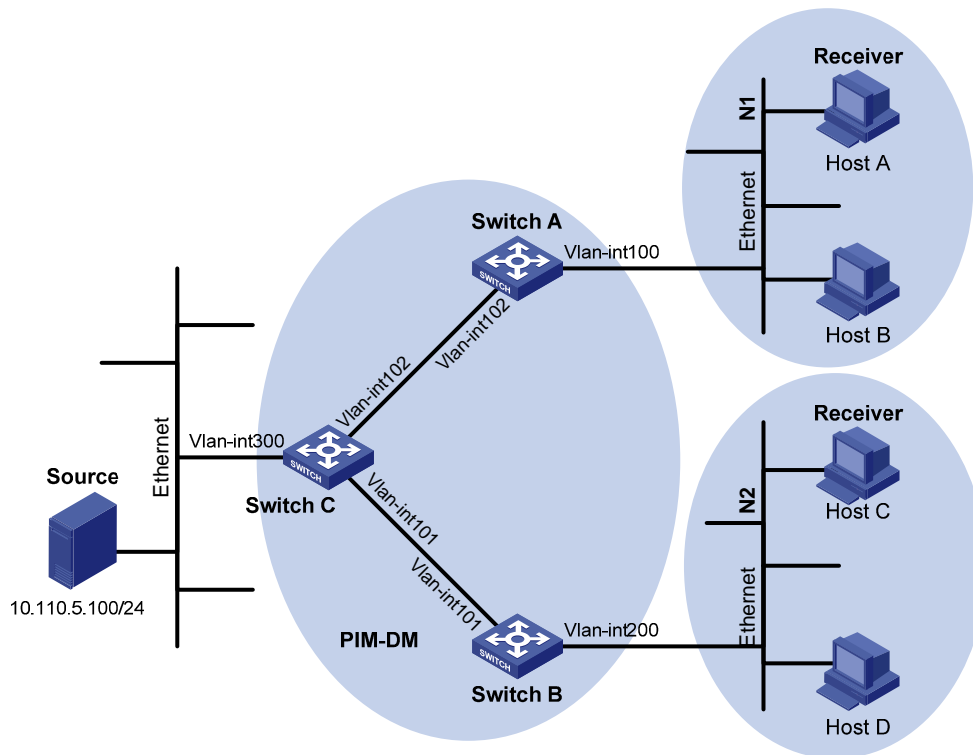


Table 13 Interface and IP address assignment

| 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 13. (Details not shown.)
2. Configure OSPF on the switches in the PIM-DM domain. (Details not shown.)

3. Enable IP multicast routing and PIM-DM:

# On Switch A, enable IP multicast routing globally.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
```

# On Switch A, enable PIM-DM on each interface.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim dm
[SwitchA-Vlan-interface102] quit
```

# On Switch B and Switch C, enable IP multicast routing and PIM-DM in the same way Switch A is configured. (Details not shown.)

4. Enable IGMPv2 on the interfaces that are directly connected to user networks:

# On Switch A, enable IGMP on VLAN-interface 100. (By default, the IGMP version is 2.)

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] quit
```

# On Switch B, enable IGMP on VLAN-interface 200 in the same way Switch A is configured. (Details not shown.)

## Verifying the configuration

1. Send IGMPv2 reports from Host A and Host C to join the multicast group **225.1.1.1**. (Details not shown.)
2. Send multicast data from the multicast source **10.110.5.100/24** to the multicast group. (Details not shown.)
3. Verify that correct PIM routing information can be created on each switch. This configuration takes Switch A and Switch C as examples:

# Display the PIM routing table on Switch C.

```
[SwitchC] display pim routing-table
VPN-Instance: public net
Total 0 (*, G) entry; 1 (S, G) entry
```

```
(10.110.5.100, 225.1.1.1)
```

```
Protocol: pim-dm, Flag: LOC ACT
UpTime: 00:03:27
Upstream interface: Vlan-interface300
 Upstream neighbor: NULL
 RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 2
 1: Vlan-interface101
```

```
Protocol: pim-dm, UpTime: 00:03:27, Expires: never
2: Vlan-interface102
Protocol: pim-dm, UpTime: 00:03:27, Expires: never
```

# Display the PIM routing table on Switch A.

```
[SwitchA] display pim routing-table
VPN-Instance: public net
Total 1 (*, G) entry; 1 (S, G) entry
```

```
(*, 225.1.1.1)
```

```
Protocol: pim-dm, Flag: WC
UpTime: 00:04:25
Upstream interface: NULL
Upstream neighbor: NULL
RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface100
Protocol: igmp, UpTime: 00:04:25, Expires: never
```

```
(10.110.5.100, 225.1.1.1)
```

```
Protocol: pim-dm, Flag: ACT
UpTime: 00:06:14
Upstream interface: Vlan-interface102,
Upstream neighbor: 192.168.1.2
RPF prime neighbor: 192.168.1.2
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface100
Protocol: pim-dm, UpTime: 00:04:25, Expires: never
```

The output shows that:

- An SPT has been established through traffic flooding. Switches on the SPT path have their (S, G) entries.
- Because Host A sends an IGMP report to Switch A to join the multicast group G, a (\*, G) entry is generated on Switch A.

## Configuration files

- Switch A:

```
#
multicast routing-enable
#
vlan 100
#
vlan 102
#
interface Vlan-interface100
```

```
ip address 10.110.1.1 255.255.255.0.
igmp enable
pim dm
#
interface Vlan-interface102
ip address 192.168.1.1 255.255.255.0
pim dm
#
ospf 1
area 0.0.0.0
network 10.110.1.0 0.0.0.255
network 192.168.1.0 0.0.0.255
#
```

- **Switch B:**

```
#
multicast routing-enable
#
vlan 101
#
vlan 200
#
interface Vlan-interface101
ip address 192.168.2.1 255.255.255.0.
pim dm
#
interface Vlan-interface200
ip address 10.110.2.1 255.255.255.0
igmp enable
pim dm
#
ospf 1
area 0.0.0.0
network 10.110.2.0 0.0.0.255
network 192.168.2.0 0.0.0.255
#
```

- **Switch C:**

```
#
multicast routing-enable
#
vlan 101 to 102
#
vlan 300
#
interface Vlan-interface101
ip address 192.168.2.2 255.255.255.0.
pim dm
#
interface Vlan-interface102
```



```
ip address 192.168.1.2 255.255.255.0
pim dm
#
interface Vlan-interface300
ip address 10.110.5.1 255.255.255.0
pim dm
#
ospf 1
area 0.0.0.0
network 10.110.5.0 0.0.0.255
network 192.168.1.0 0.0.0.255
network 192.168.2.0 0.0.0.255
#
```

## Example: Configuring PIM-SM

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

### Network requirements

As shown in [Figure 159](#):

- All the switches are Layer 3 switches, and they run OSPF.
- The multicast source, receiver hosts, and switches can communicate with each other through unicast routes.

Configure PIM-SM on each switch so that multicast data of the multicast groups in the range of **225.1.1.0/24** can be sent to receivers in **N1** and **N2**.

Figure 159 Network diagram

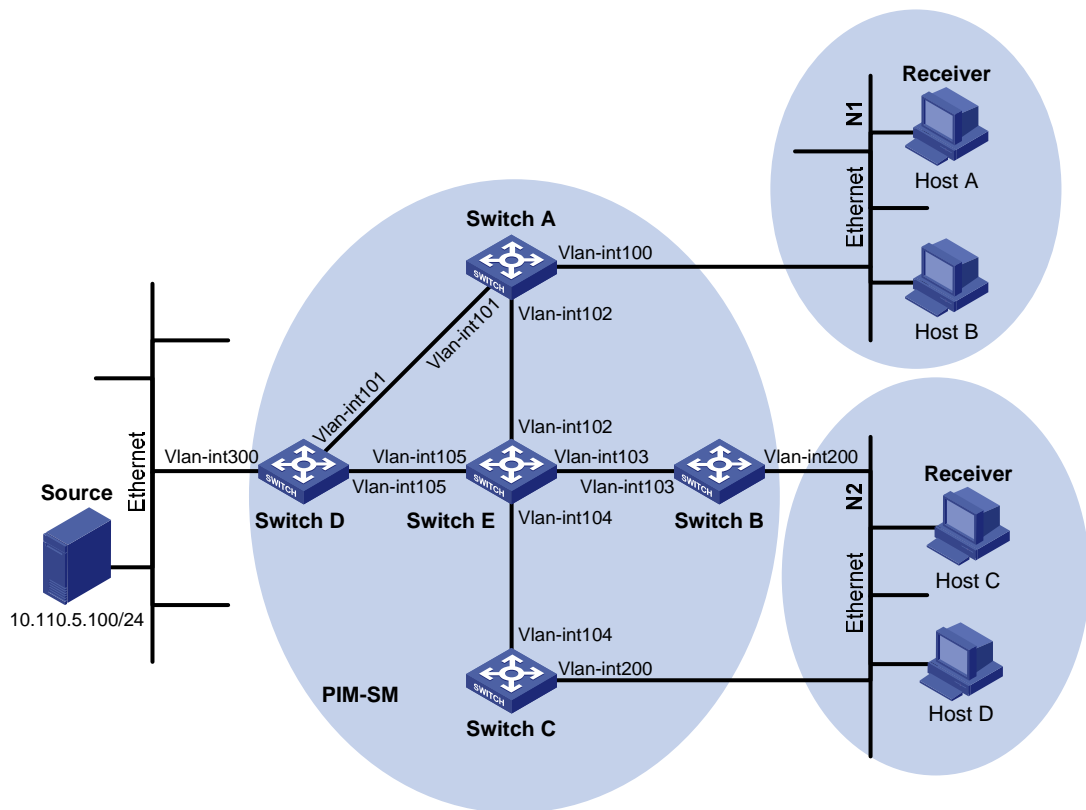


Table 14 Interface and IP address assignment

| 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

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, configure IGMP and PIM-SM on each Layer 3 switch to avoid communication interruption. In this way, 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 14](#). (Details not shown.)
2. Enable OSPF on all switches on the PIM-SM network. (Details not shown.)
3. Enable IP multicast routing and PIM-SM:

# On Switch A, enable IP multicast routing globally.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
```

# On Switch A, enable PIM-SM on each interface.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim sm
```

```
[SwitchA-Vlan-interface102] quit
```

# On Switch B, Switch C, Switch D, and Switch E, enable IP multicast routing and PIM-SM in the same way Switch A is configured. (Details not shown.)

**4.** Enable IGMPv2 on the interfaces that are directly connected to stub networks:

# On Switch A, enable IGMP on VLAN-interface 100. (By default, the IGMP version is 2.)

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] quit
```

# On Switch B and Switch C, enable IGMP on VLAN-interface 200 in the same way Switch A is configured. (Details not shown.)

**5.** Configure C-BSRs and C-RPs:

# On Switch D, create an ACL to define a multicast group range to which the C-RP is designated.

```
<SwitchD> system-view
[SwitchD] acl number 2005
[SwitchD-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[SwitchD-acl-basic-2005] quit
```

# On Switch D, configure VLAN-interface 105 as a C-RP. Reference ACL 2005 to provide services for only the multicast groups in the range of **225.1.1.0/24**.

```
[SwitchD] pim
[SwitchD-pim] c-rp vlan-interface 105 group-policy 2005
```

# On Switch D, configure VLAN-interface 105 as a C-BSR, and set its hash mask length and priority to 32 and 10, respectively.

```
[SwitchD-pim] c-bsr vlan-interface 105 32 10
[SwitchD-pim] quit
```

# On Switch E, create an ACL to define a multicast group range to which C-RP is designated.

```
<SwitchE> system-view
[SwitchE] acl number 2005
[SwitchE-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[SwitchE-acl-basic-2005] quit
```

# On Switch E, configure VLAN-interface 105 as a C-RP. Reference ACL 2005 to provide services for only the multicast groups in the range of **225.1.1.0/24**.

```
[SwitchE] pim
[SwitchE-pim] c-rp vlan-interface 102 group-policy 2005
```

# On Switch E, configure VLAN-interface 102 as a C-BSR. Set its hash mask length and priority to **32** and **20**, respectively.

```
[SwitchE-pim] c-bsr vlan-interface 102 32 20
[SwitchE-pim] quit
```

## Verifying the configuration

**1.** Verify that the IGMP querier and the DR are correctly elected on the shared-media network **N2**:

# Display information about the IGMP querier election on Switch B.

```
[SwitchB] display igmp interface
Interface information of VPN-Instance: public net
Vlan-interface200(10.110.2.1):
 IGMP is enabled
 Current IGMP version is 2
 Value of query interval for IGMP(in seconds): 60
 Value of other querier present interval for IGMP(in seconds): 125
 Value of maximum query response time for IGMP(in seconds): 10
 Querier for IGMP: 10.110.2.1 (this router)
 Total 1 IGMP Group reported
```

# Display information about the IGMP querier election on Switch C.

```
[SwitchC] display igmp interface
Interface information of VPN-Instance: public net
Vlan-interface200(10.110.2.2):
 IGMP is enabled
 Current IGMP version is 2
 Value of query interval for IGMP(in seconds): 60
 Value of other querier present interval for IGMP(in seconds): 125
 Value of maximum query response time for IGMP(in seconds): 10
 Querier for IGMP: 10.110.2.1
 Total 1 IGMP Group reported
```

The output shows that Switch B is elected 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
VPN-Instance: public net
Interface NbrCnt HelloInt DR-Pri DR-Address
Vlan103 1 30 1 192.168.2.2
Vlan200 1 30 1 10.110.2.2
```

# Display PIM information on Switch C.

```
[SwitchC] display pim interface
VPN-Instance: public net
Interface NbrCnt HelloInt DR-Pri DR-Address
Vlan104 1 30 1 192.168.3.2
Vlan200 1 30 1 10.110.2.2 (local)
```

The output shows that Switch C is elected 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. (Details not shown.)
  - c. Display PIM routing table information on the switches. This configuration takes Switch A, Switch C, and Switch D as examples:

# Display the PIM routing table on Switch A.

```
[SwitchA] display pim routing-table
```

```
VPN-Instance: public net
```

```
Total 1 (*, G) entry; 1 (S, G) entry
```

```
(*, 225.1.1.1)
```

```
RP: 192.168.9.2
```

```
Protocol: pim-sm, Flag: WC
```

```
UpTime: 00:13:46
```

```
Upstream interface: Vlan-interface102,
```

```
Upstream neighbor: 192.168.9.2
```

```
RPF prime neighbor: 192.168.9.2
```

```
Downstream interface(s) information:
```

```
Total number of downstreams: 1
```

```
1: Vlan-interface100
```

```
Protocol: igmp, UpTime: 00:13:46, Expires:00:03:06
```

```
(10.110.5.100, 225.1.1.1)
```

```
RP: 192.168.9.2
```

```
Protocol: pim-sm, Flag: SPT ACT
```

```
UpTime: 00:00:42
```

```
Upstream interface: Vlan-interface101,
```

```
Upstream neighbor: 192.168.1.2
```

```
RPF prime neighbor: 192.168.1.2
```

```
Downstream interface(s) information:
```

```
Total number of downstreams: 1
```

```
1: Vlan-interface100
```

```
Protocol: pim-sm, UpTime: 00:00:42, Expires:00:03:06
```

# Display the PIM routing table on Switch D.

```
[SwitchD] display pim routing-table
```

```
VPN-Instance: public net
```

```
Total 0 (*, G) entry; 1 (S, G) entry
```

```
(10.110.5.100, 225.1.1.1)
```

```
RP: 192.168.9.2
```

```
Protocol: pim-sm, Flag: SPT ACT
```

```
UpTime: 00:00:42
```

```
Upstream interface: Vlan-interface300
```

```
Upstream neighbor: NULL
```

```
RPF prime neighbor: NULL
```

```
Downstream interface(s) information:
```

```
Total number of downstreams: 1
```

```
1: Vlan-interface101
```

```
Protocol: pim-sm, UpTime: 00:00:42, Expires:00:02:06
```

# Display the PIM routing table on Switch E.

```
[SwitchE] display pim routing-table
```

```
VPN-Instance: public net
```

```
Total 1 (*, G) entry; 1 (S, G) entry
```

```
(*, 225.1.1.1)
```

```
RP: 192.168.9.2 (local)
```

```
Protocol: pim-sm, Flag: WC
```

```
UpTime: 00:13:16
```

```
Upstream interface: Register
```

```
Upstream neighbor: NULL
```

```
RPF prime neighbor: NULL
```

```
Downstream interface(s) information:
```

```
Total number of downstreams: 1
```

```
1: Vlan-interface102
```

```
Protocol: pim-sm, UpTime: 00:13:16, Expires: 00:03:22
```

```
(10.110.5.100, 225.1.1.1)
```

```
RP: 192.168.9.2 (local)
```

```
Protocol: pim-sm, Flag: RPT SPT ACT
```

```
UpTime: 00:25:32
```

```
Upstream interface: Vlan-interface105
```

```
Upstream neighbor: 192.168.4.2
```

```
RPF prime neighbor: 192.168.4.2
```

```
Downstream interface(s) information: None
```

The output shows that:

- The RP for the multicast group **225.1.1.1** is Switch E based on the hash calculation.
- An SPT has been built between the source-side DR (Switch D) and the RP (Switch E).
- An RPT has been built between the receiver-side DR (Switch A) and the RP (Switch E), and Switch A and Switch E have created (\*, G) entries. After receiving multicast data, the receiver-side DR (Switch A) immediately switches from the RPT to the SPT.

A new SPT is built between the receiver-side DR (Switch A) and the source-side DR (Switch D). The switches (Switch A and Switch D) on the new SPT path have their (S, G) entries.

## Configuration files

- Switch A:

```
#
multicast routing-enable
#
vlan 100 to 102
#
interface Vlan-interface100
ip address 10.110.1.1 255.255.255.0
igmp enable
pim sm
#
interface Vlan-interface101
```

```
ip address 192.168.1.1 255.255.255.0
pim sm
#
interface Vlan-interface102
ip address 192.168.9.1 255.255.255.0
pim sm
#
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
network 192.168.9.0 0.0.0.255
network 10.110.1.0 0.0.0.255
#
```

- **Switch B:**

```
#
multicast routing-enable
#
vlan 103
#
vlan 200
#
interface Vlan-interface103
ip address 192.168.2.1 255.255.255.0
pim sm
#
interface Vlan-interface200
ip address 10.110.2.1 255.255.255.0
igmp enable
pim sm
#
ospf 1
area 0.0.0.0
network 192.168.2.0 0.0.0.255
network 10.110.2.0 0.0.0.255
#
```

- **Switch C:**

```
#
multicast routing-enable
#
vlan 104
#
vlan 200
#
interface Vlan-interface104
ip address 192.168.3.1 255.255.255.0
pim sm
#
interface Vlan-interface200
```



```
ip address 10.110.2.2 255.255.255.0
igmp enable
pim sm
#
ospf 1
area 0.0.0.0
network 192.168.3.0 0.0.0.255
network 10.110.2.0 0.0.0.255
#
```

- Switch D:

```
#
multicast routing-enable
#
acl number 2005
rule 0 permit source 225.1.1.0 0.0.0.255
#
vlan 101
#
vlan 105
#
vlan 300
#
interface Vlan-interface101
ip address 192.168.1.2 255.255.255.0
pim sm
#
interface Vlan-interface105
ip address 192.168.4.2 255.255.255.0
pim sm
#
interface Vlan-interface300
ip address 10.110.5.1 255.255.255.0
pim sm
#
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
network 192.168.4.0 0.0.0.255
network 10.110.5.0 0.0.0.255
#
Pim
c-bsr hash-length 32
c-bsr priority 10
c-bsr Vlan-interface105
c-rp Vlan-interface105 group-policy 2005
#
```

- Switch E:

```
#
```

```

multicast routing-enable
#
acl number 2005
 rule 0 permit source 225.1.1.0 0.0.0.255
#
vlan 102 to 104
#
vlan 105
#
interface Vlan-interface102
 ip address 192.168.9.2 255.255.255.0
 pim sm
#
interface Vlan-interface103
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface Vlan-interface104
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface Vlan-interface105
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
 network 192.168.9.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
 network 192.168.3.0 0.0.0.255
 network 192.168.4.0 0.0.0.255
#
pim
 c-bsr hash-length 32
 c-bsr priority 20
 c-bsr Vlan-interface102
 c-rp Vlan-interface102 group-policy 2005
#

```

## Example: Configuring PIM-SM admin-scoped zones

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

# Network requirements

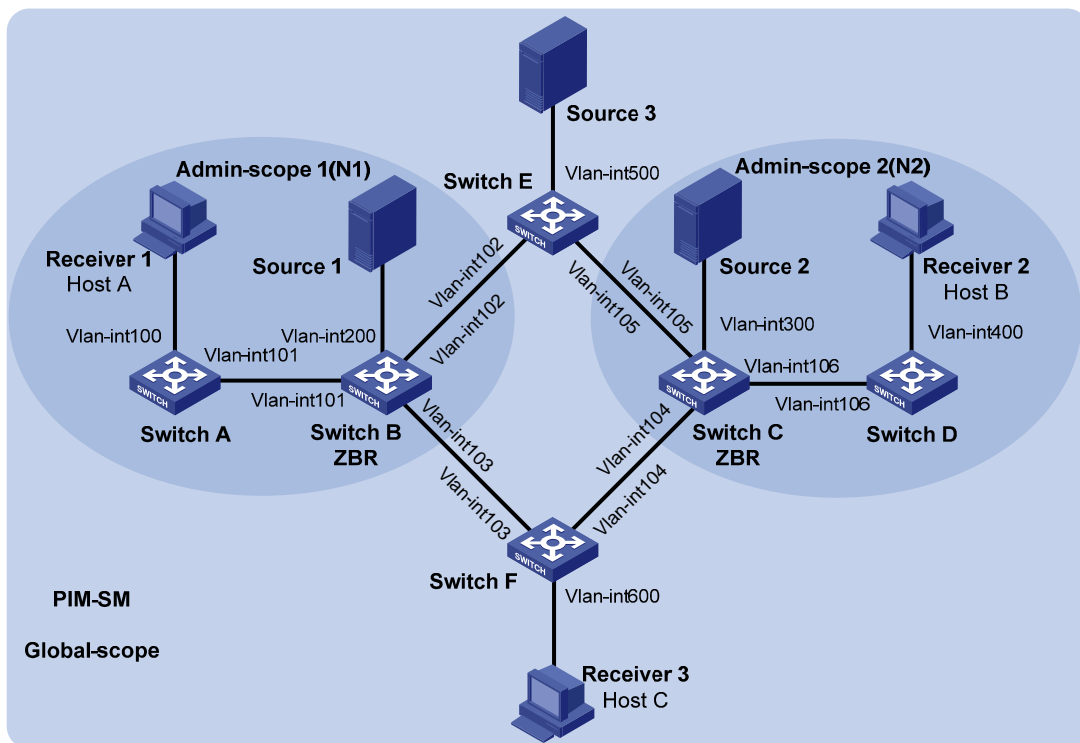
As shown in [Figure 160](#):

- All switches are Layer 3 switches, and they run OSPF.
- Multicast sources, receiver hosts, and switches can communicate with each other through unicast routes.

Use the PIM-SM administrative scoping mechanism to 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 160 Network diagram**



**Table 15 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 |

| Device   | Interface          | IP address     | Device   | Interface          | IP address      |
|----------|--------------------|----------------|----------|--------------------|-----------------|
| Switch A | VLAN-interface 101 | 10.110.1.1/24  | Switch E | VLAN-interface 500 | 192.168.5.1/24  |
| Switch B | VLAN-interface 200 | 192.168.2.1/24 | Switch E | VLAN-interface 102 | 10.110.2.2/24   |
| Switch B | VLAN-interface 101 | 10.110.1.2/24  | Switch E | VLAN-interface 105 | 10.110.5.2/24   |
| Switch B | VLAN-interface 102 | 10.110.2.1/24  | Switch F | VLAN-interface 600 | 192.168.6.1/24  |
| Switch B | VLAN-interface 103 | 10.110.3.1/24  | Switch F | VLAN-interface 103 | 10.110.3.2/24   |
| Switch C | VLAN-interface 300 | 192.168.3.1/24 | Switch F | VLAN-interface 104 | 10.110.4.2/24   |
| Switch C | VLAN-interface 104 | 10.110.4.1/24  | Source 1 | N/A                | 192.168.2.10/24 |
| Switch C | VLAN-interface 105 | 10.110.5.1/24  | Source 2 | N/A                | 192.168.3.10/24 |
| Switch C | VLAN-interface 106 | 10.110.6.1/24  | Source 3 | N/A                | 192.168.5.10/24 |
| Switch D | VLAN-interface 400 | 192.168.4.1/24 |          |                    |                 |

## Requirements analysis

To divide different admin-scoped zones, 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.
- Before you configure admin-scoped zones, enable administrative scoping on all Layer 3 switches in the PIM-SM domain.
- When you use the **multicast boundary** command to specify the multicast groups to which the admin-scoped zone is designated, the groups 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 15](#). (Details not shown.)

2. Enable OSPF on all the switches on the PIM-SM network. (Details not shown.)

3. Enable IP multicast routing, administrative scoping, IGMP, and PIM-SM:

# On Switch A, enable IP multicast routing globally.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
```

# On Switch A, enable administrative scoping.

```
[SwitchA] pim
[SwitchA-pim] c-bsr admin-scope
[SwitchA-pim] quit
```

# On Switch A, enable PIM-SM on each interface.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
```

# On Switch B, Switch C, Switch D, Switch E, and Switch F, enable IP multicast routing, administrative scoping, and PIM-SM in the same way Switch A is configured. (Details not shown.)

# On Switch A, enable IGMP on VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface101] quit
```

# On Switch D and Switch F, enable IGMP in the same way Switch A is configured. (Details not shown.)

4. Configure admin-scoped zone boundaries:

# On Switch B, configure VLAN-interface 102 and VLAN-interface 103 as the boundaries of admin-scoped zone 1.

```
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] multicast boundary 239.0.0.0 8
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] multicast boundary 239.0.0.0 8
[SwitchB-Vlan-interface103] quit
```

# On Switch C, configure VLAN-interface 104 and VLAN-interface 105 as the boundaries of admin-scoped zone 2.

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 104
[SwitchC-Vlan-interface104] multicast boundary 239.0.0.0 8
```

```
[SwitchC-Vlan-interface104] quit
[SwitchC] interface vlan-interface 105
[SwitchC-Vlan-interface105] multicast boundary 239.0.0.0 8
[SwitchC-Vlan-interface105] quit
```

## 5. Configure C-BSRs and C-RPs:

# On Switch B, create an ACL to define a multicast group range to which the C-RP is designated. .

```
[SwitchB] acl number 2001
[SwitchB-acl-basic-2001] rule permit source 239.0.0.0 0.255.255.255
[SwitchB-acl-basic-2001] quit
```

# On Switch B, configure VLAN-interface 101 as a C-RP. Reference ACL 2001 to provide services for only the multicast groups in the range of **239.0.0.0/8**.

```
[SwitchB] pim
[SwitchB-pim] c-rp vlan-interface 101 group-policy 2001
```

# On Switch B, configure VLAN-interface 101 as a C-BSR for admin-scoped zone 1.

```
[SwitchB-pim] c-bsr group 239.0.0.0 8
[SwitchB-pim] c-bsr vlan-interface 101
[SwitchB-pim] quit
```

# On Switch C, create an ACL to define a multicast group range to which the C-RP is designated.

```
[SwitchC] acl number 2001
[SwitchC-acl-basic-2001] rule permit source 239.0.0.0 0.255.255.255
[SwitchC-acl-basic-2001] quit
```

# On Switch C, configure VLAN-interface 106 as a C-RP. Reference ACL 2001 to provide services for only the multicast groups in the range of **239.0.0.0/8**.

```
[SwitchC] pim
[SwitchC-pim] c-rp vlan-interface 106 group-policy 2001
```

# On Switch C, configure VLAN-interface 106 as a C-BSR for admin-scoped zone 2.

```
[SwitchC-pim] c-bsr group 239.0.0.0 8
[SwitchC-pim] c-bsr vlan-interface 106
[SwitchC-pim] quit
```

# On Switch E, configure VLAN-interface 102 as a C-BSR and a C-RP for the global-scoped zone.

```
<SwitchE> system-view
[SwitchE] pim
[SwitchE-pim] c-bsr global
[SwitchE-pim] c-bsr vlan-interface 102
[SwitchE-pim] c-rp vlan-interface 102
[SwitchE-pim] quit
```

## Verifying the configuration

1. Verify that the BSR has been elected and that the local C-RP configuration in each zone has taken effect:

# Display information about the BSR and the locally configured C-RP on Switch B.

```
[SwitchB] display pim bsr-info
VPN-Instance: public net
```

```

Elected BSR Address: 10.110.2.2
 Priority: 64
 Hash mask length: 30
 State: Accept Preferred
 Scope: Global
 Uptime: 00:01:45
 Expires: 00:01:25
Elected BSR Address: 10.110.1.2
 Priority: 64
 Hash mask length: 30
 State: Elected
 Scope: 239.0.0.0/8
 Uptime: 00:04:54
 Next BSR message scheduled at: 00:00:06
Candidate BSR Address: 10.110.1.2
 Priority: 64
 Hash mask length: 30
 State: Elected
 Scope: 239.0.0.0/8

Candidate RP: 10.110.1.2(Vlan-interface101)
 Priority: 192
 HoldTime: 150
 Advertisement Interval: 60
 Next advertisement scheduled at: 00:00:15

```

# Display information about the BSR and the locally configured C-RP on Switch C.

```

[SwitchC] display pim bsr-info
VPN-Instance: public net
Elected BSR Address: 10.110.2.2
 Priority: 64
 Hash mask length: 30
 State: Accept Preferred
 Scope: Global
 Uptime: 00:01:45
 Expires: 00:01:25
Elected BSR Address: 10.110.6.1
 Priority: 64
 Hash mask length: 30
 State: Elected
 Scope: 239.0.0.0/8
 Uptime: 00:03:48
 Next BSR message scheduled at: 00:01:12
Candidate BSR Address: 10.110.6.1
 Priority: 64
 Hash mask length: 30
 State: Elected
 Scope: 239.0.0.0/8

```

```
Candidate RP: 10.110.6.1(Vlan-interface106)
 Priority: 192
 HoldTime: 150
 Advertisement Interval: 60
 Next advertisement scheduled at: 00:00:10
```

# Display information about the BSR and the locally configured C-RP on Switch E.

```
[SwitchE] display pim bsr-info
VPN-Instance: public net
Elected BSR Address: 10.110.2.2
 Priority: 64
 Hash mask length: 30
 State: Elected
 Scope: Global
 Uptime: 00:11:11
 Next BSR message scheduled at: 00:00:49
Candidate BSR Address: 10.110.2.2
 Priority: 64
 Hash mask length: 30
 State: Elected
 Scope: Global
```

```
Candidate RP: 10.110.2.2 (Vlan-interface102)
 Priority: 192
 HoldTime: 150
 Advertisement Interval: 60
 Next advertisement scheduled at: 00:00:55
```

2. Verify that the RP has been elected in each zone to provide services for different multicast groups:

# Display RP information on Switch B.

```
[SwitchB] display pim rp-info
VPN-Instance: public net
PIM-SM BSR RP information:
Group/MaskLen: 224.0.0.0/4
 RP: 10.110.2.2
 Priority: 192
 HoldTime: 150
 Uptime: 00:03:39
 Expires: 00:01:51
```

```
Group/MaskLen: 239.0.0.0/8
 RP: 10.110.1.2 (local)
 Priority: 192
 HoldTime: 150
 Uptime: 00:07:44
 Expires: 00:01:51
```

# Display RP information on Switch C.

```
[SwitchC] display pim rp-info
VPN-Instance: public net
```



```
PIM-SM BSR RP information:
Group/MaskLen: 224.0.0.0/4
RP: 10.110.2.2
Priority: 192
HoldTime: 150
Uptime: 00:03:42
Expires: 00:01:48
```

```
Group/MaskLen: 239.0.0.0/8
RP: 10.110.6.1 (local)
Priority: 192
HoldTime: 150
Uptime: 00:06:54
Expires: 00:02:41
```

#### # Display RP information on Switch E.

```
[SwitchE] display pim rp-info
VPN-Instance: public net
PIM-SM BSR RP information:
Group/MaskLen: 224.0.0.0/4
RP: 10.110.2.2 (local)
Priority: 192
HoldTime: 150
Uptime: 00:00:32
Expires: 00:01:58
```

#### # Display RP information on Switch F.

```
[SwitchF] display pim rp-info
VPN-Instance: public net
PIM-SM BSR RP information:
Group/MaskLen: 224.0.0.0/4
RP: 10.110.2.2
Priority: 192
HoldTime: 150
Uptime: 00:04:30
Expires: 00:02:23
```

The output shows that:

- When a host in admin-scoped zone 1 joins a multicast group in the range of **239.0.0.0/8**, the RP (Switch B) provides services for this multicast group locally.
- When a host in admin-scoped zone 2 joins a multicast group in the range of **239.0.0.0/8**, the RP (Switch C) provides services for this multicast group locally.
- When a host in an admin-scoped zone or the global-scoped zone joins a multicast group out of the range of **239.0.0.0/8**, the RP (Switch E) provides services for this multicast group.

## Configuration files

- Switch A:

```

#
multicast routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 192.168.1.1 255.255.255.0
 igmp enable
 pim sm
#
interface Vlan-interface101
 ip address 10.110.1.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
 network 10.110.1.0 0.0.0.255
#
pim
 c-bsr admin-scope
#

```

- **Switch B:**

```

#
multicast routing-enable
#
acl number 2001
 rule 0 permit source 239.0.0.0 0.255.255.255
#
vlan 101 to 103
#
vlan 200
#
interface Vlan-interface101
 ip address 10.110.1.2 255.255.255.0
 pim sm
#
interface Vlan-interface102
 ip address 10.110.2.1 255.255.255.0
 multicast boundary 239.0.0.0 8
 pim sm
#
interface Vlan-interface103
 ip address 10.110.3.1 255.255.255.0
 multicast boundary 239.0.0.0 8
 pim sm
#
interface Vlan-interface200

```

```

ip address 192.168.2.1 255.255.255.0
pim sm
#
ospf 1
area 0.0.0.0
network 192.168.2.0 0.0.0.255
network 10.110.1.0 0.0.0.255
network 10.110.2.0 0.0.0.255
network 10.110.3.0 0.0.0.255
#
pim
c-bsr admin-scope
c-bsr group 239.0.0.0 255.0.0.0
c-bsr vlan-interface 101
c-rp vlan-interface 101 group-policy 2001
#

```

- Switch C:

```

#
multicast routing-enable
#
acl number 2001
rule 0 permit source 239.0.0.0 0.255.255.255
#
vlan 104 to 106
#
vlan 300
#
interface Vlan-interface104
ip address 10.110.4.1 255.255.255.0
multicast boundary 239.0.0.0 8
pim sm
#
interface Vlan-interface105
ip address 10.110.5.1 255.255.255.0
multicast boundary 239.0.0.0 8
pim sm
#
interface Vlan-interface106
ip address 10.110.6.1 255.255.255.0
pim sm
#
interface Vlan-interface300
ip address 192.168.3.1 255.255.255.0
pim sm
#
ospf 1
area 0.0.0.0
network 192.168.3.0 0.0.0.255

```

```

network 10.110.4.0 0.0.0.255
network 10.110.5.0 0.0.0.255
network 10.110.6.0 0.0.0.255
#
pim
c-bsr admin-scope
c-bsr group 239.0.0.0 255.0.0.0
c-bsr vlan-interface 106
c-rp vlan-interface 106 group-policy 2001
#

```

- Switch D:

```

#
multicast routing-enable
#
vlan 106
#
vlan 400
#
interface Vlan-interface106
ip address 10.110.6.2 255.255.255.0
pim sm
#
interface Vlan-interface400
ip address 192.168.4.1 255.255.255.0
igmp enable
pim sm
#
ospf 1
area 0.0.0.0
network 192.168.4.0 0.0.0.255
network 10.110.6.0 0.0.0.255
#
pim
c-bsr admin-scope
#

```

- Switch E:

```

#
multicast routing-enable
#
vlan 102
#
vlan 105
#
vlan 500
#
interface Vlan-interface102
ip address 10.110.2.2 255.255.255.0
pim sm

```

```

#
interface Vlan-interface105
 ip address 10.110.5.2 255.255.255.0
 pim sm
#
interface Vlan-interface500
 ip address 192.168.5.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
 network 192.168.5.0 0.0.0.255
 network 10.110.2.0 0.0.0.255
 network 10.110.5.0 0.0.0.255
#
pim
 c-bsr admin-scope
 c-bsr global
 c-bsr vlan-interface 102
 c-rp vlan-interface 102
#

```

- Switch F:

```

#
multicast routing-enable
#
vlan 103 to 104
#
vlan 600
#
interface Vlan-interface103
 ip address 10.110.3.2 255.255.255.0
 pim sm
#
interface Vlan-interface104
 ip address 10.110.4.2 255.255.255.0
 pim sm
#
interface Vlan-interface600
 ip address 192.168.6.1 255.255.255.0
 igmp enable
 pim sm
#
ospf 1
 area 0.0.0.0
 network 192.168.6.0 0.0.0.255
 network 10.110.3.0 0.0.0.255
 network 10.110.4.0 0.0.0.255
#

```

```
pim
c-bsr admin-scope
#
```

## Example: Configuring PIM-SSM

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

### Network requirements

As shown in [Figure 161](#):

- All switches are Layer 3 switches, and they run OSPF.
- Multicast sources, receiver hosts, and switches can communicate with each other through unicast routes.
- The receiver hosts in the user networks support IGMPv3.

Configure PIM-SSM on each switch, so that the receiver hosts can receive VOD streams destined for a multicast group in the SSM group range **232.1.1.0/24** from a specific multicast source.

Figure 161 Network diagram

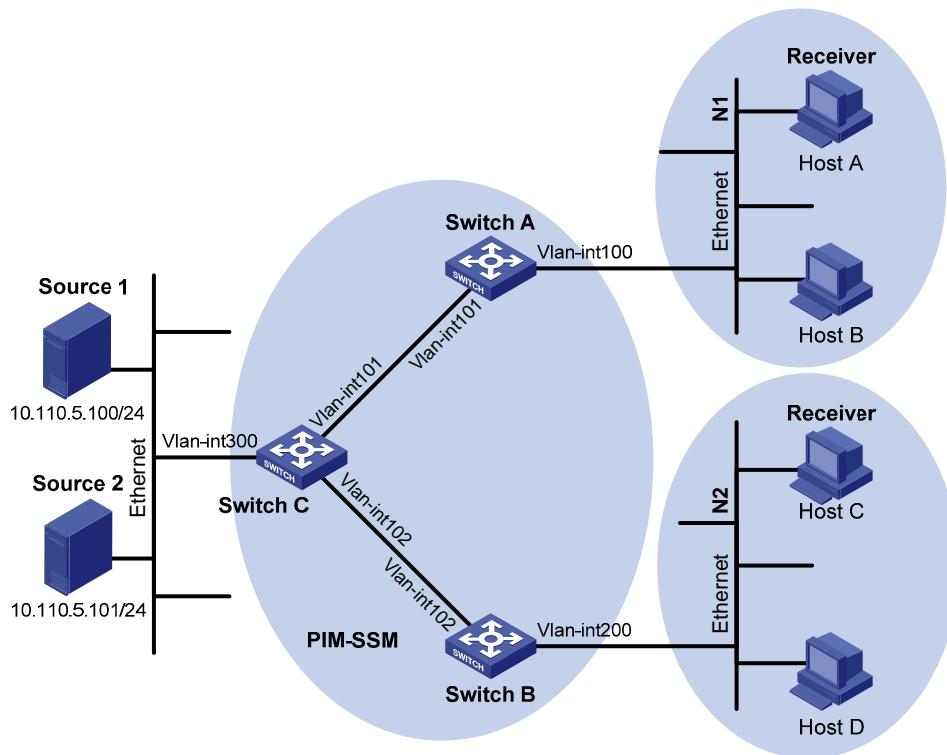


Table 16 Interface and IP address assignment

| 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 B | VLAN-interface 200 | 10.110.2.1/24  |
| Switch B | VLAN-interface 102 | 192.168.2.1/24 |
| Switch C | VLAN-interface 300 | 10.110.5.1/24  |
| Switch C | VLAN-interface 101 | 192.168.1.2/24 |
| Switch C | VLAN-interface 102 | 192.168.2.2/24 |

## Requirements analysis

To enable PIM-SSM to provide services for multicast groups in the range specified in the network requirements, you must specify this range on each Layer 3 switch.

In SSM, the edge Layer 3 switch must get information about the specified multicast source when a host joins a multicast group. You must enable IGMPv3 on the edge switches that connect to the user networks.

## Configuration restrictions and guidelines

When a member of a multicast group in the SSM group range sends an IGMPv1 or IGMPv2 report message, the switch does not trigger a (\*, G) join message. You can configure IGMP SSM mappings, so that PIM-SSM can provide services for hosts that support IGMPv1 or IGMPv2.

## Configuration procedures

1. Assign an IP address and subnet mask to each interface according to [Table 16](#). (Details not shown.)

2. Configure OSPF on the switches in the PIM-SSM domain. (Details not shown.)

3. Enable IP multicast routing and PIM-SSM on each switch:

# On Switch A, enable IP multicast routing globally.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
```

# On Switch A, enable PIM-SM on each interface.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
```

# On Switch B and Switch C, enable IP multicast routing and PIM-SM in the same way Switch A is configured. (Details not shown.)

4. Configure the SSM group range:

# On Switch A, configure the SSM group range to be **232.1.1.0/24**.

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[SwitchA-acl-basic-2000] quit
[SwitchA] pim
[SwitchA-pim] ssm-policy 2000
[SwitchA-pim] quit
```

# On Switch B and Switch C, configure the SSM group range in the same way Switch A is configured. (Details not shown.)

5. Enable IGMPv3 on the interfaces that are directly connected to user networks:

# On Switch A, enable IGMPv3 on VLAN-interface 100. (By default, the IGMP version is 2.)

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] igmp version 3
[SwitchA-Vlan-interface100] quit
```



# On Switch B, enable IGMPv3 on VLAN-interface 200 in the same way Switch A is configured. (Details not shown.)

## Verifying the configuration

1. Send an IGMPv3 report from Host A to join the multicast group **232.1.1.1** and specify the multicast source as **10.110.5.100/24**. (Details not shown.)
2. Verify that correct (S, G) entries can be created on each switch. This configuration takes Switch A and Switch C as examples:

# Display the PIM routing table on Switch A.

```
[SwitchA] display pim routing-table
VPN-Instance: public net
Total 1 (S, G) entry
```

```
(10.110.5.100, 232.1.1.1)
```

```
Protocol: pim-ssm, Flag:
UpTime: 00:13:25
Upstream interface: Vlan-interface101
 Upstream neighbor: 192.168.1.2
 RPF prime neighbor: 192.168.1.2
Downstream interface(s) information:
 Total number of downstreams: 1
 1: Vlan-interface100
 Protocol: igmp, UpTime: 00:13:25, Expires: -
```

# Display the PIM routing table on Switch C.

```
[SwitchC] display pim routing-table
VPN-Instance: public net
Total entry; 1 (S, G) entry
```

```
(10.110.5.100, 232.1.1.1)
```

```
Protocol: pim-ssm, Flag:LOC
UpTime: 00:12:05
Upstream interface: Vlan-interface300
 Upstream neighbor: NULL
 RPF prime neighbor: NULL
Downstream interface(s) information:
 Total number of downstreams: 1
 1: Vlan-interface101
 Protocol: pim-ssm, UpTime: 00:12:05, Expires: 00:03:25
```

The output shows that Switch A builds an SPT toward the multicast source. Switches on the SPT path (Switch A and Switch D) generate (S, G) entries.

# Configuration files

- Switch A:

```
#
multicast routing-enable
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 10.110.1.1 255.255.255.0
 igmp enable
 igmp version 3
 pim sm
#
interface Vlan-interface101
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
 network 10.110.1.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
#
pim
 ssm-policy 2000
#
```
- Switch B:

```
#
multicast routing-enable
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
vlan 102
#
vlan 200
#
interface Vlan-interface102
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface Vlan-interface200
 ip address 10.110.2.1 255.255.255.0
 igmp enable
```

```

 igmp version 3
 pim sm
 #
 ospf 1
 area 0.0.0.0
 network 10.110.2.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
 #
 pim
 ssm-policy 2000
 #
 • Switch C:
 #
 multicast routing-enable
 #
 acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
 #
 vlan 101 to 102
 #
 vlan 300
 #
 interface Vlan-interface101
 ip address 192.168.1.2 255.255.255.0
 pim sm
 #
 interface Vlan-interface102
 ip address 192.168.2.2 255.255.255.0
 pim sm
 #
 interface Vlan-interface300
 ip address 10.110.5.1 255.255.255.0
 pim sm
 #
 ospf 1
 area 0.0.0.0
 network 10.110.5.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
 #
 pim
 ssm-policy 2000
 #

```

# Port isolation configuration examples

This chapter provides port isolation configuration examples.

The port isolation feature isolates Layer 2 traffic for data privacy and security without using VLANs. You can also use this feature to isolate the hosts in a VLAN from one another.

## Example: Configuring port isolation

### Applicable product matrix

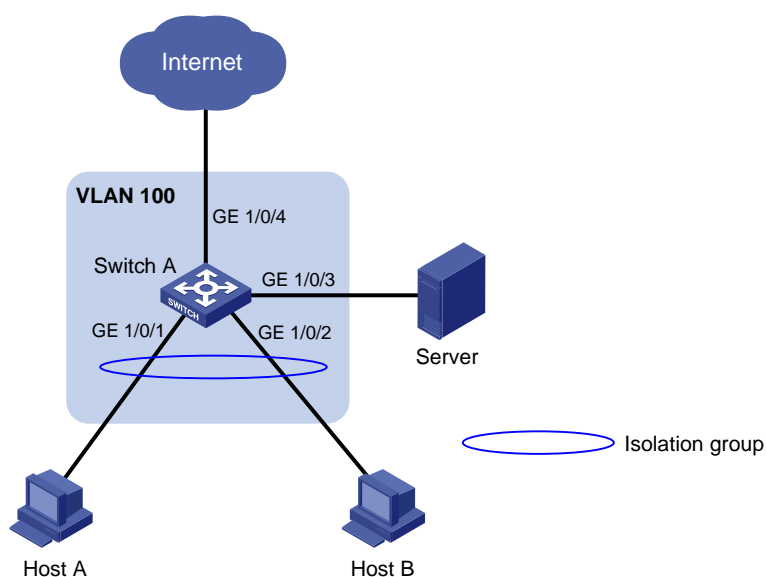
| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

### 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 GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to the VLAN.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-vlan100] quit
```

# Assign ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the isolation group.

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

## Verifying the configuration

# Display information about the isolation group.

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

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
vlan 100
#
interface GigabitEthernet1/0/1
port link-mode bridge
port access vlan 100
port-isolate enable
```

```

#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 port-isolate enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#

```

## Example: Implementing time-based access control for isolated ports

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

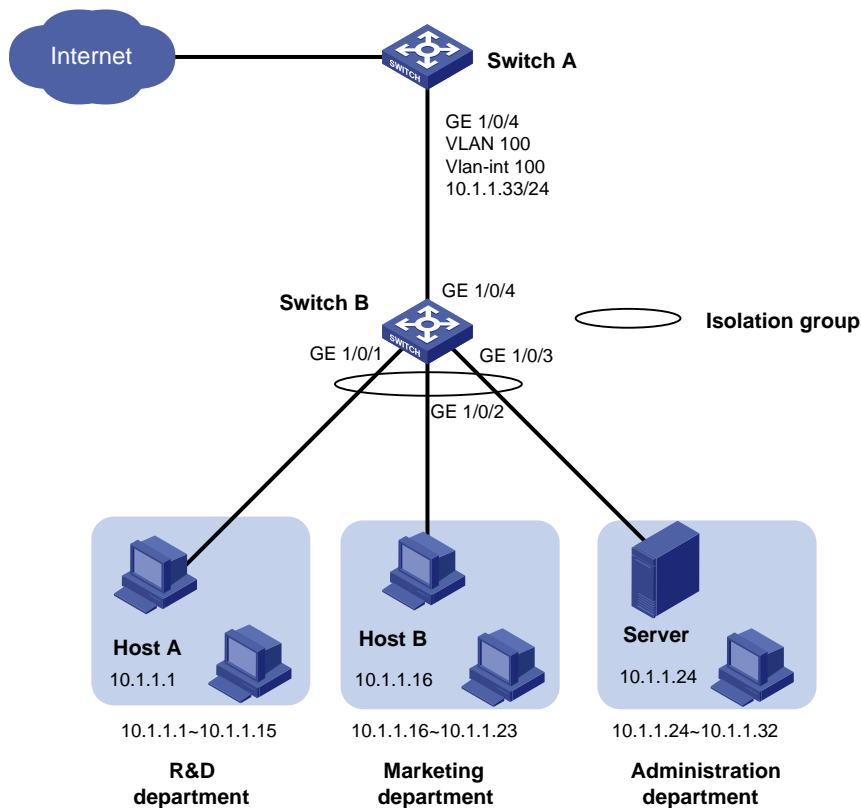
### Network requirements

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 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

### Configuring Switch B

```
Add ports GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and
GigabitEthernet 1/0/4 to VLAN 100.
```

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchB-vlan100] quit
```

```
Assign ports GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 to
the isolation group to disable host A and host B from accessing the server at Layer 2.
```

```
[SwitchB] interface gigabitethernet 1/0/1
```

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

## Configuring Switch A

# Configure the IP address and mask of VLAN-interface 100.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/4
[SwitchA-vlan100] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.1.1.33 255.255.255.0
```

# Enable local proxy ARP on VLAN-interface 100 to enable host A and host B to access the server at Layer 3.

```
[SwitchA-Vlan-interface100] local-proxy-arp enable
[SwitchA-Vlan-interface100] quit
```

# Create two periodic time ranges: **trname\_1** and **trname\_2**. **trname\_1** is active from 8:00 to 12:00 every day. **trname\_2** is active from 14:00 to 16:00 every day.

```
[SwitchA] time-range trname_1 8:00 to 12:00 daily
[SwitchA] time-range trname_2 14:00 to 16:00 daily
```

# Create IPv4 ACL 3000.

```
[SwitchA] acl number 3000
```

# Configure one rule to permit access from host A to the server from 8:00 to 12:00 every day.

```
[SwitchA-acl-adv-3000] rule permit ip source 10.1.1.1 0 destination 10.1.1.24 0
time-range trname_1
```

# Configure one rule to permit access from host B to the server from 14:00 to 16:00 every day.

```
[SwitchA-acl-adv-3000] rule permit ip source 10.1.1.16 0 destination 10.1.1.24 0
time-range trname_2
```

# Configure one rule to deny all cross-department communications.

```
[SwitchA-acl-adv-3000] rule deny ip source 10.1.1.0 0.0.0.31 destination 10.1.1.0
0.0.0.31
[SwitchA-acl-adv-3000] quit
```

# Apply the IPv4 advanced ACL 3000 to GigabitEthernet 1/0/4 to filter incoming packets.

```
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] packet-filter 3000 inbound
```

## Verifying the configuration

# Display information about the isolation group on Switch B.

```
[SwitchB] display port-isolate group
Port-isolate group information:
```



```

Uplink port support: NO
Group ID: 1
Group members:
 GigabitEthernet1/0/1 GigabitEthernet1/0/2 GigabitEthernet1/0/3

Display information about VLAN 100 on Switch A.
[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 on Switch A.
[SwitchA]display acl 3000
Advanced ACL 3000, named -none-, 3 rules,
ACL's step is 5
 rule 0 permit ip source 10.1.1.1 0 destination 10.1.1.24 0 time-range trname_1
 rule 5 permit ip source 10.1.1.16 0 destination 10.1.1.24 0 time-range trname_2
 rule 10 deny ip source 10.1.1.0 0.0.0.31 destination 10.1.1.0 0.0.0.31

```

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch B:

```

#
vlan 100
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
 port-isolate enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 port-isolate enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
 port-isolate enable
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#

```

- Switch A:

```
#
time-range trname_1_8:00 to 12:00 daily
time-range trname_2 14:00 to 16:00 daily
#
acl number 3000
rule 0 permit ip source 10.1.1.1 0 destination 10.1.1.24 0 time-range trname_1
rule 5 permit ip source 10.1.1.16 0 destination 10.1.1.24 0 time-range trname_2
rule 10 deny ip source 10.1.1.0 0.0.0.31 destination 10.1.1.0 0.0.0.31
#
vlan 100
#
interface Vlan-interface 100
ip address 10.1.1.33 255.255.255.0
local-proxy-arp enable
#
interface GigabitEthernet1/0/4
port link-mode bridge
port access vlan 100
packet-filter 3000 inbound
#
```

# Port security configuration examples

This chapter provides examples for configuring port security modes to control network access of users.

## General configuration restrictions and guidelines

When you configure port security, follow these restrictions and guidelines:

- Disable global 802.1X and MAC authentications before you enable port security on a port.
- When port security is enabled, you cannot manually enable 802.1X or MAC authentication, change the access control mode, or change the port authorization state. The port security feature provides a group of port security modes. It modifies these settings automatically when you change the port security mode.
- 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

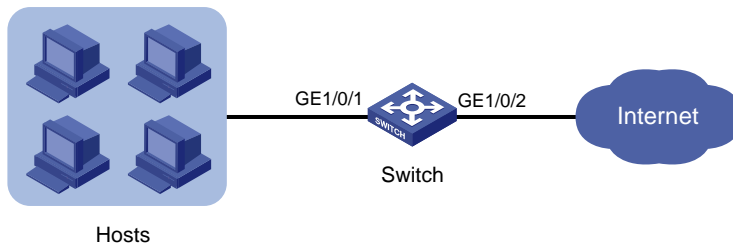
| Product series | Software version    |
|----------------|---------------------|
| HP 5500 EI     | Release series 2220 |
| HP 5500 SI     |                     |

### 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 coming users to access the Internet.

Figure 164 Network diagram



## Requirements analysis

Because the hosts are connected to GigabitEthernet 1/0/1, configure the autoLearn mode on that port.

To update MAC address table, configure an aging timer for the secure MAC addresses. This example uses 30 minutes.

To deny any new coming users to access the Internet after the number of online users reaches 64, enable intrusion traps and configure the port to shut down temporarily for 30 seconds.

## Configuration restrictions and guidelines

When you configure the autoLearn mode, follow these restrictions and guidelines:

- To change the security mode of a port security-enabled port, 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

# Enter system view.

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

# 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 GigabitEthernet 1/0/1.

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
```

# Set the port security mode to **autoLearn**.

```
[Switch-GigabitEthernet1/0/1] port-security port-mode autolearn
```

# Configure the port to be silent for 30 seconds after the intrusion protection feature is triggered.

```
[Switch-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Switch-GigabitEthernet1/0/1] quit
[Switch] port-security timer disableport 30
```

# Enable intrusion traps and port security. The port security module sends traps when it detects illegal frames.

```
[Switch] port-security trap intrusion
[Switch] port-security enable
Please wait..... Done.
```

## Verifying the configuration

# Display the port security configuration.

```
<Switch> display port-security interface gigabitethernet 1/0/1
Equipment port-security is enabled
Intrusion trap is enabled
AutoLearn aging time is 30 minutes
Disableport Timeout: 30s
OUI value:
```

```
GigabitEthernet1/0/1 is link-up
Port mode is autoLearn
NeedToKnow mode is disabled
Intrusion Protection mode is DisablePortTemporarily
Max MAC address number is 64
Stored MAC address number is 0
Authorization is permitted
Security MAC address learning mode is sticky
Security MAC address aging type is absolute
```

The output shows the following:

- The port security's limit on the number of secure MAC addresses on the port is 64.
- The port security mode is autoLearn.
- The intrusion protection action is disabling the port (DisablePortTemporarily) for 30 seconds.

The port allows for MAC address learning, and you can view the number of learned MAC addresses in the message "Stored MAC address number is n".

# Use the **display port-security** command repeatedly to track the number of MAC addresses learned by the port.

# Use the **display this** command in interface view to display the learned secure MAC addresses.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
port link-mode bridge
```

```

port-security max-mac-count 64
port-security port-mode autolearn
port-security intrusion-mode disableport-temporarily
port-security mac-address security sticky 0002-0000-0015 vlan 1
port-security mac-address security sticky 0002-0000-0014 vlan 1
port-security mac-address security sticky 0002-0000-0013 vlan 1
port-security mac-address security sticky 0002-0000-0012 vlan 1
port-security mac-address security sticky 0002-0000-0011 vlan 1
#

```

Use the **display port-security interface** command after the number of MAC addresses learned by the port reaches 64. You can see that the port security mode is changed to **secure**. When a frame with an unknown MAC address arrives, intrusion protection is triggered. The following trap is sent:

```

#Apr 26 12:47:14:210 2000 Switch PORTSEC/4/VIOLATION:
Trap1.3.6.1.4.1.25506.2.26.1.3.2
 An intrusion occurs!
 IfIndex: 17825797
 Port: 17825797
 MAC Addr: E8:39:35:5F:31:91
 VLAN ID: 1
 IfAdminStatus: 2

```

# Use the **display interface** command. The output shows that the port is disabled.

```

<Switch> display interface gigabitethernet 1/0/1
 gigabitEthernet1/0/1 current state: DOWN (Port Security Disabled)
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0023-8927-ad7d
 Description: GigabitEthernet1/0/1 Interface

```

# Use the **display interface** command after 30 seconds. The output shows that the interface is enabled.

```

[Switch-GigabitEthernet1/0/1] display interface gigabitethernet 1/0/1
 GigabitEthernet1/0/1 current state: UP
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
 Description: GigabitEthernet1/0/1 Interface


```

# Use the **undo port-security mac-address security** command to delete several secure MAC addresses. The port security mode of the port changes to **autoLearn**, and the port can learn MAC addresses again.

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```

#
port-security enable
port-security trap intrusion
port-security timer autolearn aging 30
port-security timer disableport 30
#
interface GigabitEthernet1/0/1
port link-mode bridge

```

```

port-security max-mac-count 64
port-security port-mode autolearn
port-security intrusion-mode disableport-temporarily
#

```

## Example: Configuring userLoginWithOUI mode

### Applicable product matrix

| Product series | Software version    |
|----------------|---------------------|
| HP 5500 EI     | Release series 2220 |
| HP 5500 SI     |                     |

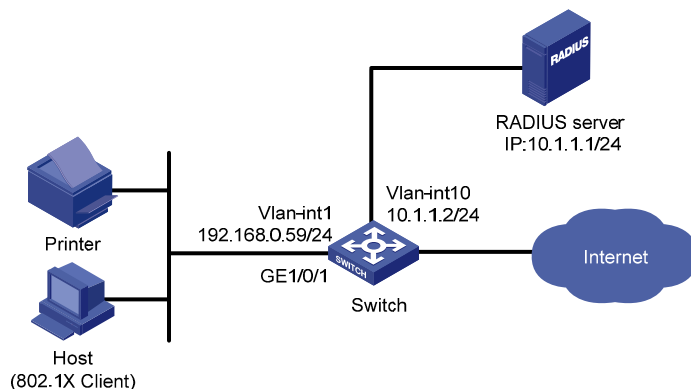
### Network requirements

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, and it discards all frames sourced from the blocked MAC addresses.

**Figure 165 Network diagram**



## Requirements analysis

Because the hosts are connected to GigabitEthernet 1/0/1, configure the userLoginWithOUI mode on that port.

To permit the printer to access the Internet, add the OUI of the printer to the switch. To match the OUIs of different printer vendors, add multiple OUIs to the switch.

To perform RADIUS-based authentication, configure a RADIUS scheme and specify an authentication domain.

## Configuration restrictions and guidelines

When you configure the userLoginWithOUI mode, follow these restrictions and guidelines:

- To change the security mode of a port security-enabled port, use the **undo port-security port-mode** command to set the port in noRestrictions mode first.
- The authentication port (UDP) used by RADIUS servers is 1812 according to standard RADIUS protocols. However, the port (UDP) is set to 1645 on an HP device that functions as the RADIUS authentication server. You must specify the authentication port as **1645** in the RADIUS scheme on the switch.

## Configuration procedures

This example uses the HP 5500 HI switch as the RADIUS server. For more information about configuring the RADIUS server, see *HP 5500 HI 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. Specify the RADIUS server at 10.1.1.1 as the primary authentication server. Set the shared key for authentication to aabbcc.
```

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

```
[Switch] radius scheme radsun
```

```
New Radius scheme
```

```
[Switch-radius-radsun] primary authentication 10.1.1.1 1645 key aabbcc
```

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

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

```
Set the maximum number of RADIUS packet retransmission attempts to 5.
```

```
[Switch-radius-radsun] retry 5
```



```

Configure the switch to send usernames without domain names to the RADIUS server.
[Switch-radius-radsun] user-name-format without-domain
[Switch-radius-radsun] quit

Create ISP domain sun and enter ISP domain view.
[Switch] domain sun
[Switch-isp-sun]

Configure ISP domain sun to use RADIUS scheme radsun for authentication and authorization of
all LAN-access users.
[Switch-isp-sun] authentication default radius-scheme radsun
[Switch-isp-sun] authorization default radius-scheme radsun
[Switch-isp-sun] accounting default none
[Switch-isp-sun] quit

```

2. Set the 802.1X authentication method to CHAP. By default, the authentication method is CHAP for 802.1X.

```

[Switch] dot1x authentication-method chap
CHAP authentication enabled already.

```

3. Configure port security:

```

Add five OUI values.

```

```

[Switch] port-security oui 1234-0100-1111 index 1
[Switch] port-security oui 1234-0200-1111 index 2
[Switch] port-security oui 1234-0300-1111 index 3
[Switch] port-security oui 1234-0400-1111 index 4
[Switch] port-security oui 1234-0500-1111 index 5

```

```

Set the port security mode to userLoginWithOUI.

```

```

[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui

```

```

Configure port GigabitEthernet 1/0/1 to perform the blockmac intrusion protection feature.

```

```

[Switch-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
[Switch-GigabitEthernet1/0/1] quit

```

```

Enable port security.

```

```

[Switch] port-security enable
Please wait..... Done.

```

## Configuring the RADIUS server

```

Create RADIUS user aaa on the RADIUS server, and enter RADIUS-server user view.

```

```

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

```

```

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

```

```

[Sysname-rdsuser-aaa] password simple 123456
[Sysname-rdsuser-aaa] quit

```

```

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

```

```

[Sysname] radius-server client-ip 10.1.1.2 key simple aabbcc

```

## Verifying the configuration

# Display the RADIUS scheme **radsun**.

```
[Switch] display radius scheme radsun
SchemeName : radsun
 Index : 1 Type : standard
 Primary Auth Server:
 IP: 10.1.1.1 Port: 1645 State: active
 Encryption Key : *****
 VPN instance : N/A
 Probe username : N/A
 Probe interval : N/A
 Auth Server Encryption Key : N/A
 Acct Server Encryption Key : N/A
 VPN instance : N/A
 Accounting-On packet disable, send times : 50 , interval : 3s
 Interval for timeout(second) : 5
 Retransmission times for timeout : 5
 Interval for realtime accounting(minute) : 12
 Retransmission times of realtime-accounting packet : 5
 Retransmission times of stop-accounting packet : 500
 Quiet-interval(min) : 5
 Username format : without-domain
 Data flow unit : Byte
 Packet unit : one
```

# Display the configuration of the ISP domain **sun**.

```
<Switch> display domain sun
 Domain: sun
 State: Active
 Access-limit: Disabled
 Accounting method: Required
 Default authentication scheme : radius:radsun
 Default authorization scheme : radius:radsun
 Default accounting scheme : none
 Domain User Template:
 Idle-cut : Disabled
 Self-service : Disabled
 Authorization attributes:
```

# Display the port security configuration.

```
<Switch> display port-security interface gigabitethernet 1/0/1
 Equipment port-security is enabled
 Trap is disabled
 AutoLearn aging time is 0 minutes
 Disableport Timeout: 20s
 OUI value:
 Index is 1, OUI value is 123401
```

Index is 2, OUI value is 123402  
Index is 3, OUI value is 123403  
Index is 4, OUI value is 123404  
Index is 5, OUI value is 123405

GigabitEthernet1/0/1 is link-up  
Port mode is userLoginWithOUI  
NeedToKnow mode is disabled  
Intrusion Protection mode is BlockMacAddress  
Max MAC address number is not configured  
Stored MAC address number is 0  
Authorization is permitted  
Security MAC address learning mode is sticky  
Security MAC address aging type is absolute

After an 802.1X user goes online, the number of secure MAC addresses saved by the port is 1.

#### # Display 802.1X information.

```
<Switch> display dot1x interface gigabitethernet 1/0/1
```

Equipment 802.1X protocol is enabled  
CHAP authentication is enabled  
Proxy trap checker is disabled  
Proxy logoff checker is disabled  
EAD quick deploy is disabled

Configuration: Transmit Period 30 s, Handshake Period 15 s  
Quiet Period 60 s, Quiet Period Timer is disabled  
Supp Timeout 30 s, Server Timeout 100 s  
Reauth Period 3600 s  
The maximal retransmitting times 2

EAD quick deploy configuration:

EAD timeout: 30 m

Total maximum 802.1X user resource number is 1024 per slot  
Total current used 802.1X resource number is 1

GigabitEthernet1/0/1 is link-up  
802.1X protocol is enabled  
Proxy trap checker is disabled  
Proxy logoff checker is disabled  
Handshake is enabled  
Handshake secure is disabled  
802.1X unicast-trigger is enabled  
Periodic reauthentication is disabled  
The port is an authenticator  
Authentication Mode is Auto  
Port Control Type is Mac-based  
802.1X Multicast-trigger is enabled  
Mandatory authentication domain: NOT configured

```

Guest VLAN: NOT configured
Auth-Fail VLAN: NOT configured
Critical VLAN: NOT configured
Critical recovery-action: NOT configured
Max number of on-line users is 256

EAPOL Packet: Tx 16331, Rx 102
Sent EAP Request/Identity Packets : 16316
 EAP Request/Challenge Packets: 6
 EAP Success Packets: 4, Fail Packets: 5
Received EAPOL Start Packets : 6
 EAPOL LogOff Packets: 2
 EAP Response/Identity Packets : 80
 EAP Response/Challenge Packets: 6
 Error Packets: 0
1. Authenticated user : MAC address: 0002-0000-0011

Controlled User(s) amount to 1

```

The port also allows an additional user whose MAC address has an OUI from the specified OUIs to pass authentication.

# Display the MAC address information for interface GigabitEthernet 1/0/1.

```

<Switch> display mac-address interface gigabitethernet 1/0/1
MAC ADDR VLAN ID STATE PORT INDEX AGING TIME(s)
1234-0300-0011 1 Learned GigabitEthernet1/0/1 AGING

--- 1 mac address(es) found ---

```

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```

#
port-security enable
port-security oui 1234-0100-0000 index 1
port-security oui 1234-0200-0000 index 2
port-security oui 1234-0300-0000 index 3
port-security oui 1234-0400-0000 index 4
port-security oui 1234-0500-0000 index 5
#
radius scheme radsun
primary authentication 10.1.1.1 1645 key cipher c3$krBjik3mdDkyVGW9JRInyID3GMYJOW==
timer response-timeout 5
user-name-format without-domain
retry 5
#
domain sun
authentication default radius-scheme radsun

```

```

authorization default radius-scheme radsun
accounting default none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
interface GigabitEthernet1/0/1
port link-mode bridge
port-security port-mode userlogin-withouti
port-security intrusion-mode blockmac
#

```

## Example: Configuring macAddressOrUserLoginSecure mode

### Applicable product matrix

| Product series | Software version    |
|----------------|---------------------|
| HP 5500 EI     | Release series 2220 |
| HP 5500 SI     |                     |

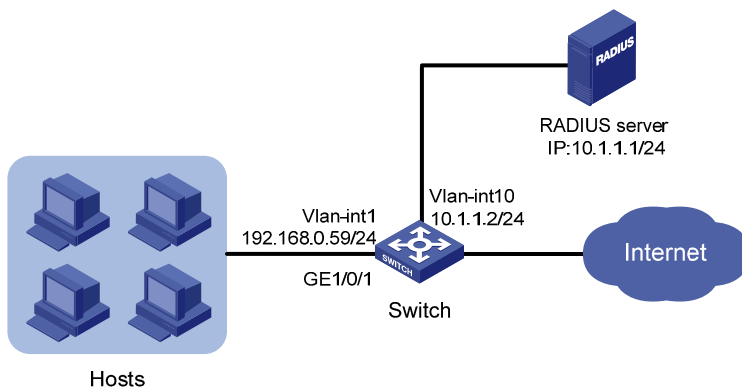
### Network requirements

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

Because the hosts are connected to GigabitEthernet 1/0/1 of the switch, configure the `macAddressOrUserLoginSecure` mode on that port.

To perform RADIUS-based authentication, configure a RADIUS scheme and specify an authentication domain.

## Configuration restrictions and guidelines

When you configure the `macAddressOrUserLoginSecure` mode, follow these restrictions and guidelines:

- To change the security mode of a port security-enabled port, use the **`undo port-security port-mode`** command to set the port in `noRestrictions` mode first.
- The authentication port (UDP) used by RADIUS servers is 1812 according to standard RADIUS protocols. However, the port (UDP) is set to 1645 on an HP device that functions as the RADIUS authentication server. You must specify the authentication port as **1645** in the RADIUS scheme on the switch.

## Configuration procedures

This example uses the HP 5500 HI switch as the RADIUS server. For more information about configuring the RADIUS server, see *HP 5500 HI 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**. Specify the RADIUS server at 10.1.1.1 as the primary authentication server. Set the shared key for authentication to **aabbcc**.

```
<Switch> system-view
[Switch] radius scheme radsun
New Radius scheme
[Switch-radius-radsun] primary authentication 10.1.1.1 1645 key aabbcc
```

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

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

# Set the maximum number of RADIUS packet retransmission attempts to 5.

```
[Switch-radius-radsun] retry 5
```

# Configure the switch to send usernames without domain names to the RADIUS server.

```
[Switch-radius-radsun] user-name-format without-domain
[Switch-radius-radsun] quit
```

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

```
[Switch] domain sun
[Switch-isp-sun]
```

# Configure ISP domain **sun** to use RADIUS scheme **radsun** for authentication and authorization of all LAN-access users.

```
[Switch-isp-sun] authentication 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 is CHAP for 802.1X.

```
[Switch] dot1x authentication-method chap
CHAP authentication enabled already.
```

# Specify ISP domain **sun** for MAC authentication.

```
[Switch] mac-authentication domain sun
```

# Configure the username and password for MAC authentication as **aaa** and **123456**.

```
[Switch] mac-authentication user-name-format fixed account aaa password simple 123456
```

# Set port security's limit on the number of secure MAC addresses to 64 on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
```

# Set the port security mode to **macAddressOrUserLoginSecure**.

```
[Switch-GigabitEthernet1/0/1] port-security port-mode userlogin-secure-or-mac
```

# Set the NTK mode of the port to **ntkonly**.

```
[Switch-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
[Switch-GigabitEthernet1/0/1] quit
```

# Enable port security.

```
[Switch] port-security enable
Please wait..... Done.
```

## Configuring the RADIUS server

# Create RADIUS user **aaa** on the RADIUS server, and enter RADIUS-server user view.

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

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

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

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

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

## Verifying the configuration

# Display the port security configuration.

```
<Switch> display port-security interface gigabitethernet 1/0/1
Equipment port-security is enabled
Trap is disabled
AutoLearn aging time is 0 minutes
Disableport Timeout: 20s
OUI value:
```

```
GigabitEthernet1/0/1 is link-up
Port mode is macAddressOrUserLoginSecure
NeedToKnow mode is NeedToKnowOnly
Intrusion Protection mode is NoAction
Max MAC address number is 64
Stored MAC address number is 0
Authorization is permitted
Security MAC address learning mode is sticky
Security MAC address aging type is absolute
```

# Display MAC authentication information.

```
<Switch> display mac-authentication interface gigabitethernet 1/0/1
MAC address authentication is enabled.
User name format is fixed account
Fixed username:aaa
Fixed password: *****
Offline detect period is 300s
Quiet period is 60s
Server response timeout value is 100s
The max allowed user number is 1024 per slot
Current user number amounts to 3
Current domain is sun
```

Silent MAC User info:

| MAC Addr | From Port | Port Index |
|----------|-----------|------------|
|----------|-----------|------------|



GigabitEthernet1/0/1 is link-up  
MAC address authentication is enabled  
Authenticate success: 3, failed: 1  
Max number of on-line users is 256  
Current online user number is 32

| MAC Addr       | Authenticate State        | Auth Index |
|----------------|---------------------------|------------|
| 1234-0300-0011 | MAC_AUTHENTICATOR_SUCCESS | 13         |
| 1234-0300-0012 | MAC_AUTHENTICATOR_SUCCESS | 14         |
| 1234-0300-0013 | MAC_AUTHENTICATOR_SUCCESS | 15         |

# Display 802.1X authentication information.

<Switch> display dot1x interface gigabitethernet 1/0/1  
Equipment 802.1X protocol is enabled  
CHAP authentication is enabled  
Proxy trap checker is disabled  
Proxy logoff checker is disabled  
EAD quick deploy is disabled

Configuration: Transmit Period 30 s, Handshake Period 15 s  
Quiet Period 60 s, Quiet Period Timer is disabled  
Supp Timeout 30 s, Server Timeout 100 s  
Reauth Period 3600 s  
The maximal retransmitting times 2  
EAD quick deploy configuration:  
EAD timeout: 30 m

The maximum 802.1X user resource number is 1024 per slot  
Total current used 802.1X resource number is 1

GigabitEthernet1/0/1 is link-up  
802.1X protocol is enabled  
Proxy trap checker is disabled  
Proxy logoff checker is disabled  
Handshake is enabled  
Handshake secure is disabled  
802.1X unicast-trigger is enabled  
Periodic reauthentication is disabled  
The port is an authenticator  
Authentication Mode is Auto  
Port Control Type is Mac-based  
802.1X Multicast-trigger is enabled  
Mandatory authentication domain: NOT configured  
Guest VLAN: NOT configured  
Auth-Fail VLAN: NOT configured  
Critical VLAN: NOT configured  
Critical recovery-action: NOT configured  
Max number of on-line users is 256

```

EAPOL Packet: Tx 16331, Rx 102
Sent EAP Request/Identity Packets : 16316
 EAP Request/Challenge Packets: 6
 EAP Success Packets: 4, Fail Packets: 5
Received EAPOL Start Packets : 6
 EAPOL LogOff Packets: 2
 EAP Response/Identity Packets : 80
 EAP Response/Challenge Packets: 6
 Error Packets: 0
1. Authenticated user : MAC address: 0002-0000-0011

```

Controlled User(s) amount to 1

Because NTK is enabled, frames with an unknown destination MAC address, multicast address, or broadcast address are discarded.

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```

#
port-security enable
#
mac-authentication domain sun
mac-authentication user-name-format fixed account aaa password cipher
c3$6DXUG/ZZMl7AbkMpJEo2uonil9WCI0nJGw
#
radius scheme radsun
primary authentication 10.1.1.1 1645 key cipher c3$krBjik3mdDkyVGW9JRInyID3GMYJOw==
timer response-timeout 5
user-name-format without-domain
retry 5
#
domain sun
authentication lan-access radius-scheme radsun
authorization lan-access radius-scheme radsun
accounting lan-access none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
interface GigabitEthernet1/0/1
port link-mode bridge
port-security max-mac-count 64
port-security port-mode userlogin-secure-or-mac
port-security ntk-mode ntkonly
#

```

# QinQ configuration examples

This chapter provides examples for using QinQ to extend customer VLANs (CVLANs) across an Ethernet service provider network.

QinQ enables service providers to separate or aggregate customer traffic in the service provider network by adding a layer of service provider VLAN tag (SVLAN tag) to customer traffic.

QinQ has the following implementations:

- **Basic QinQ**—Enabled on a per-port basis. A basic QinQ-enabled port tags all incoming frames (tagged or untagged) with the PVID tag without discriminating between CVLANs. As a result, basic QinQ cannot separate a customer's traffic by traffic type.
- **Selective QinQ**—Implemented through QoS policies or CVLAN-to-SVLAN bindings. Selective QinQ enables a port to tag incoming traffic with different SVLAN tags for different CVLANs. In contrast to basic QinQ, selective QinQ can separate traffic by both customer and traffic type.

Use basic QinQ to separate traffic by customer.

Use selective QinQ to separate traffic by CVLAN for a customer that has multiple CVLANs.

---

## NOTE:

On a QinQ-enabled port, the device learns MAC addresses to SVLANs instead of CVLANs.

---

## Example: Configuring basic QinQ

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

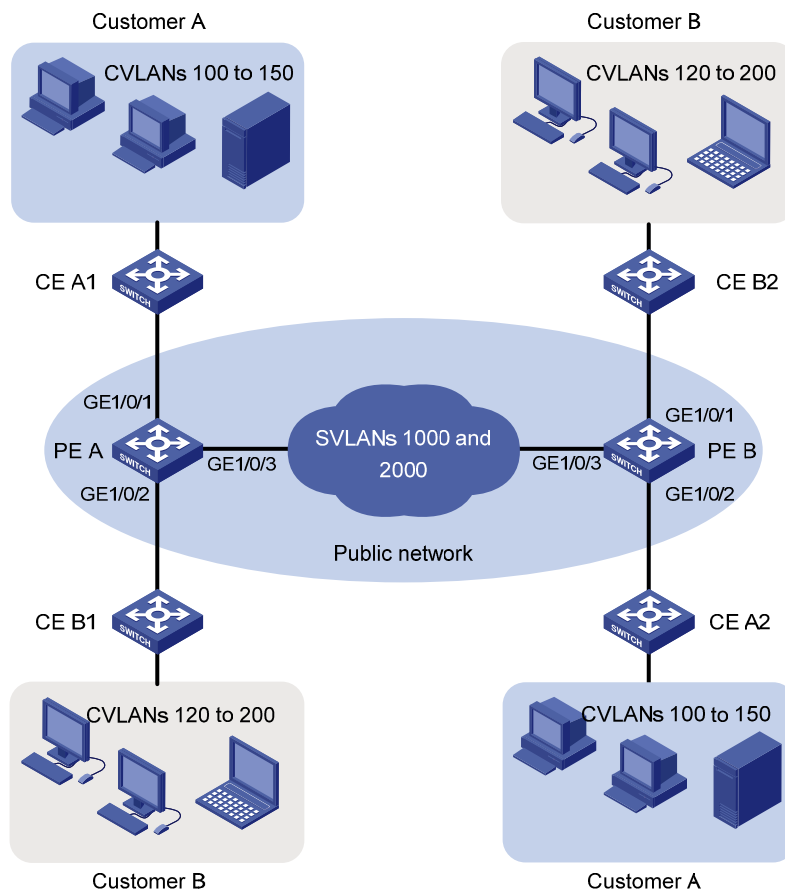
### Network requirements

As shown in [Figure 167](#), Customer A and Customer B each have two branches.

Configure basic QinQ on PE A and PE B to provide Layer 2 connectivity for Customer A and Customer B over the service provider network.

In the service provider network, assign VLAN 1000 and VLAN 2000 to Customer A and Customer B, respectively.

Figure 167 Network diagram



## Requirements analysis

To run QinQ, you only need to configure QinQ on customer-side ports of PEs.

For the customer-side hybrid ports to send traffic to the customer site with the SVLAN tag removed, you must assign the ports to the SVLANs (port VLANs) as untagged VLAN members.

For the service provider-side ports to support multiple SVLANs, configure the link type of service provider-side ports as trunk or hybrid.

To send QinQ frames across the service provider network, you must configure all the ports on the forwarding path to meet the following requirements:

- Allow frames from VLAN 1000 and VLAN 2000 to pass through.
- Retain the VLAN tags of QinQ frames.

## Configuration restrictions and guidelines

When you configure basic QinQ, follow these restrictions and guidelines:

- The link type of customer-side ports can be access, hybrid, or trunk. Basic QinQ tags incoming frames (tagged or untagged) with the PVID tag for all link types.
- You must set the SVLAN ID as the PVID on a basic QinQ-enabled port.
- You must set the MTU to at least 1504 bytes for each port on the path of QinQ frames in the service provider network.

## Configuration procedures

This example assumes that the CVLANs have been configured correctly on the CEs.

### Configuring PE A

1. Create VLAN 1000 and VLAN 2000.

```
<PE_A> system-view
[PE_A] vlan 1000
[PE_A-vlan1000] quit
[PE_A] vlan 2000
[PE_A-vlan2000] quit
```

2. Configure GigabitEthernet 1/0/1 (a customer-side port):

# Configure the port as a hybrid port, and set its PVID to 1000.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] port link-type hybrid
[PE_A-GigabitEthernet1/0/1] port hybrid pvid vlan 1000
```

# Remove the port from VLAN 1, and assign it to VLAN 1000 as an untagged VLAN member.

```
[PE_A-GigabitEthernet1/0/1] undo port hybrid vlan 1
[PE_A-GigabitEthernet1/0/1] port hybrid vlan 1000 untagged
```

# Enable basic QinQ on the port.

```
[PE_A-GigabitEthernet1/0/1] qinq enable
[PE_A-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2 (a customer-side port):

# Configure the port as an access port, and assign it to VLAN 2000.

```
[PE_A] interface gigabitethernet 1/0/2
[PE_A-GigabitEthernet1/0/2] port access vlan 2000
```

# Enable basic QinQ on the port.

```
[PE_A-GigabitEthernet1/0/2] qinq enable
[PE_A-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3 (the service provider-side port):

# Configure the port as a trunk port, and assign it to VLAN 1000 and VLAN 2000.

```
[PE_A] interface gigabitethernet 1/0/3
[PE_A-GigabitEthernet1/0/3] port link-type trunk
[PE_A-GigabitEthernet1/0/3] port trunk permit vlan 1000 2000
```

# Remove the port from VLAN 1.

```
[PE_A-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

```
[PE_A-GigabitEthernet1/0/3] quit
```

## Configuring PE B

1. Create VLAN 1000 and VLAN 2000.

```
<PE_B> system-view
[PE_B] vlan 1000
[PE_B-vlan1000] quit
[PE_B] vlan 2000
[PE_B-vlan2000] quit
```

2. Configure GigabitEthernet 1/0/1 (a customer-side port):

# Configure the port as a hybrid port, and set its PVID to 2000.

```
[PE_B] interface gigabitethernet 1/0/1
[PE_B-GigabitEthernet1/0/1] port link-type hybrid
[PE_B-GigabitEthernet1/0/1] port hybrid pvid vlan 2000
```

# Assign the port to VLAN 2000 as an untagged VLAN member, and remove it from VLAN 1.

```
[PE_B-GigabitEthernet1/0/1] port hybrid vlan 2000 untagged
[PE_B-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

# Enable basic QinQ on the port.

```
[PE_B-GigabitEthernet1/0/1] qinq enable
[PE_B-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2 (a customer-side port):

# Configure the port as an access port, and assign it to VLAN 1000.

```
[PE_B] interface gigabitethernet 1/0/2
[PE_B-GigabitEthernet1/0/2] port access vlan 1000
```

# Enable basic QinQ on the port.

```
[PE_B-GigabitEthernet1/0/2] qinq enable
[PE_B-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3 (the service provider-side port):

# Configure the port as a trunk port, and assign it to VLAN 1000 and VLAN 2000.

```
[PE_B] interface gigabitethernet 1/0/3
[PE_B-GigabitEthernet1/0/3] port link-type trunk
[PE_B-GigabitEthernet1/0/3] port trunk permit vlan 1000 2000
```

# Remove the port from VLAN 1.

```
[PE_B-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[PE_B-GigabitEthernet1/0/3] quit
```

## Configuring devices in the service provider network

# Configure all ports on the path between PE A and PE B to meet the following requirements:

- Allow frames from VLAN 1000 and VLAN 2000 to pass through.
- Retain the VLAN tags of QinQ frames.

## Verifying the configuration

# Verify the configuration on each port. For example, verify the configuration on GigabitEthernet 1/0/1 of PE A.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1000 untagged
 port hybrid pvid vlan 1000
 qinq enable
#
return
```

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- PE A:

```
#
vlan 1000
#
vlan 2000
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1000 untagged
 port hybrid pvid vlan 1000
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2000
 qinq enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1000 2000
```

- PE B:

```

#
vlan 1000
#
vlan 2000
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2000 untagged
 port hybrid pvid vlan 2000
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 1000
 qinq enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1000 2000
#

```

## Example: Configuring selective QinQ by using a QoS policy

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

### Network requirements

As shown in [Figure 168](#), Customer A and Customer B each have two branches that require Layer 2 connectivity over the service provider network.

Both customers have three types of traffic and require different transmission priorities for the three types of traffic.

Configure selective QinQ on PE A and PE B to separate the traffic by customer and traffic type, and assign different 802.1p priority values to the traffic flows.



**Figure 168 Network diagram**

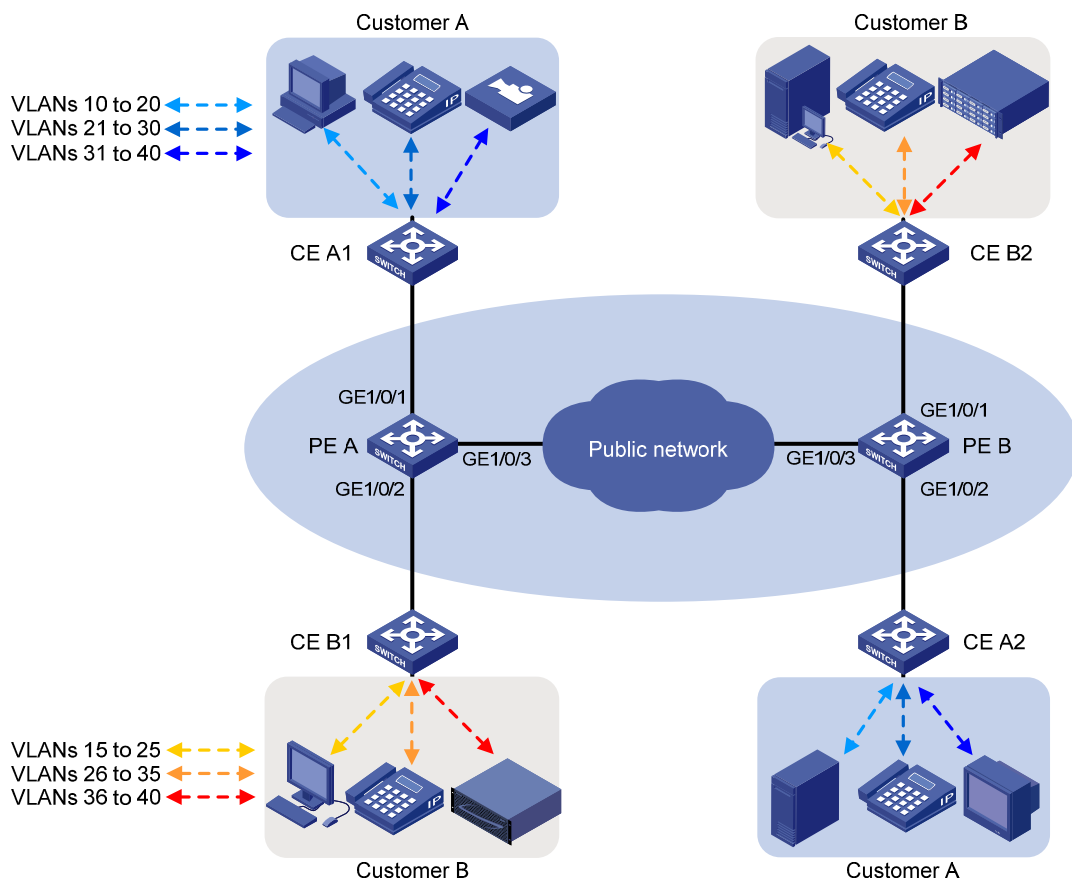
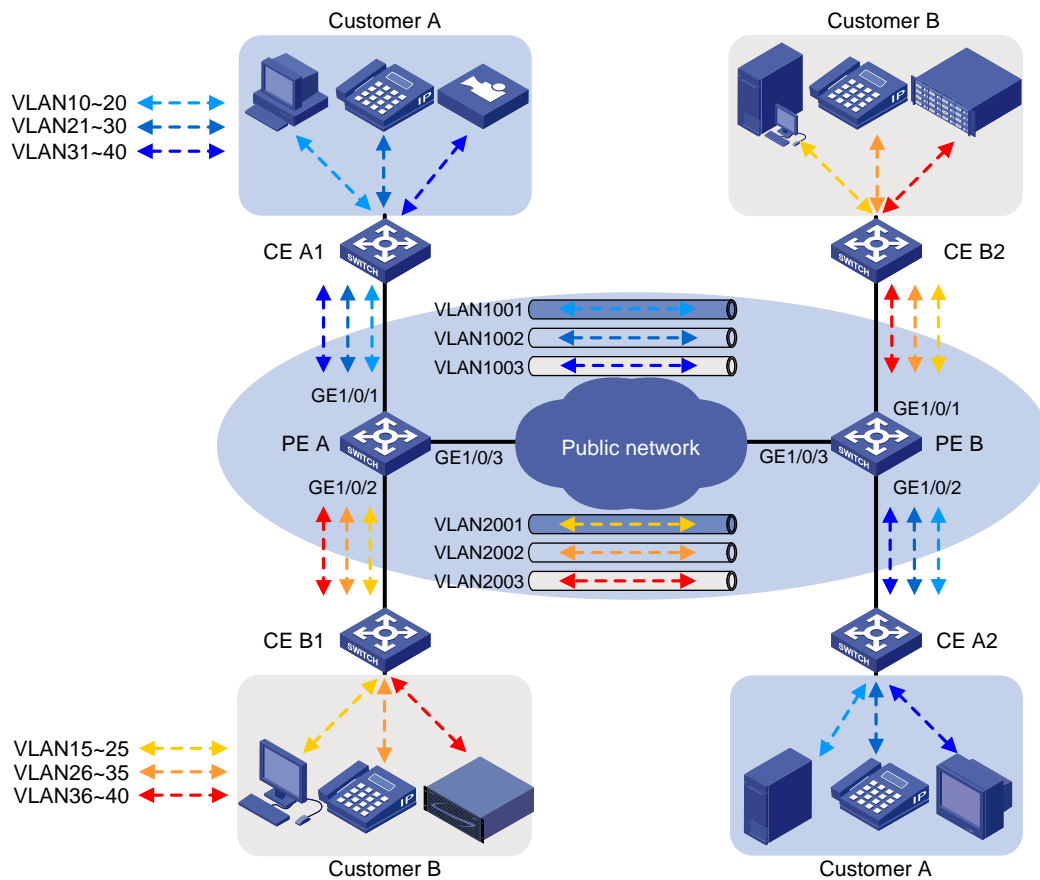


Table 17 shows the VLAN assignment scheme. For each customer, the service provider assigns one SVLAN by traffic type. Figure 169 shows the traffic transmission pattern after selective QinQ is configured.

**Table 17 VLAN assignment**

| Traffic type       | CVLANs   | SVLAN | Traffic priority |
|--------------------|----------|-------|------------------|
| <b>Customer A:</b> |          |       |                  |
| Video              | 31 to 40 | 1003  | High             |
| Voice              | 21 to 30 | 1002  | Medium           |
| Data               | 10 to 20 | 1001  | Low              |
| <b>Customer B:</b> |          |       |                  |
| Storage            | 36 to 40 | 2003  | High             |
| Voice              | 26 to 35 | 2002  | Medium           |
| Data               | 15 to 25 | 2001  | Low              |

Figure 169 Traffic pattern in the service provider network after selective QinQ is configured



## Requirements analysis

To run QinQ, you only need to configure selective QinQ on customer-side ports of PEs.

To implement selective QinQ, the customer-side ports must be hybrid ports. They must support multiple SVLANs and must send traffic to the customer site with the SVLAN tag removed.

To send QinQ frames across the service provider network, you must configure all the ports on the forwarding path to meet the following requirements:

- Allow frames from VLAN 1000 and VLAN 2000 to pass through.
- Retain the VLAN tags of QinQ frames.

## Configuration restrictions and guidelines

When you configure selective QinQ, follow these restrictions and guidelines:

- You must enable basic QinQ before applying a QoS policy that contains the next action to a port for selective QinQ.

- You can apply a QoS policy that contains the next action to the inbound direction of ports.
- If an incoming frame does not match the selective QinQ QoS policy, the port adds the PVID tag to the frame as the SVLAN tag.
- By default, the 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.
- A QinQ-enabled port cannot modify the CVLAN tag. To modify CVLAN IDs, configure CVLAN ID substitution on the service provider-side port.
- Increase the MTU to at least 1504 bytes for each port on the path of QinQ frames for forwarding QinQ frames.

## Configuration procedures

This example assumes that the CVLANs have been configured correctly on the CEs.

This example assigns SVLAN tags to frames based on CVLAN IDs. You can also base SVLAN tag assignment on other criteria such as IP addresses and MAC addresses.

### Configuring PE A

1. Create 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 GigabitEthernet 1/0/1 (a customer-side port):

# Configure the port as a hybrid port, and remove it from VLAN 1.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] port link-type hybrid
[PE_A-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

# Assign the port to SVLANs 1001 through 1003 as an untagged VLAN member.

```
[PE_A-GigabitEthernet1/0/1] port hybrid vlan 1001 to 1003 untagged
```

# Enable basic QinQ on the port.

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

# Configure the port to trust the 802.1p priority of frames.

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

3. Configure GigabitEthernet 1/0/2 (a customer-side port):

# Configure the port as a hybrid port, and remove it from VLAN 1.

```
[PE_A] interface gigabitethernet 1/0/2
[PE_A-GigabitEthernet1/0/2] port link-type hybrid
[PE_A-GigabitEthernet1/0/2] undo port hybrid vlan 1
```

# Assign the port to SVLANs 2001 through 2003 as an untagged VLAN member.

```
[PE_A-GigabitEthernet1/0/2] port hybrid vlan 2001 to 2003 untagged
```

# Enable basic QinQ on the port.

```
[PE_A-GigabitEthernet1/0/2] qinq enable
```

# Configure the port to trust the 802.1p priority of frames.

```
[PE_A-GigabitEthernet1/0/2] qos trust dot1p
```

```
[PE_A-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3 (the service provider-side port):

# Configure the port as a trunk port, and remove it from VLAN 1.

```
[PE_A] interface gigabitethernet 1/0/3
```

```
[PE_A-GigabitEthernet1/0/3] port link-type trunk
```

```
[PE_A-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

# Assign the port to SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
[PE_A-GigabitEthernet1/0/3] port trunk permit vlan 1001 to 1003 2001 to 2003
```

```
[PE_A-GigabitEthernet1/0/3] quit
```

5. Configure QoS policies for SVLAN tagging and 802.1p priority re-mark:

# Create a class named **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 for Customer A's three traffic types.

```
[PE_A] traffic behavior customer_A_pc
```

```
[PE_A-behavior-customer_A_pc] nest top-most vlan-id 1001
```

```
[PE_A-behavior-customer_A_pc] remark dot1p 3
```

```
[PE_A-behavior-customer_A_pc] quit
```

```
[PE_A] traffic behavior customer_A_voice
```

```
[PE_A-behavior-customer_A_voice] nest top-most vlan-id 1002
```

```
[PE_A-behavior-customer_A_voice] remark dot1p 5
```

```
[PE_A-behavior-customer_A_voice] quit
```

```
[PE_A] traffic behavior customer_A_video
```

```
[PE_A-behavior-customer_A_video] nest top-most vlan-id 1003
```

```
[PE_A-behavior-customer_A_video] remark dot1p 7
```

```
[PE_A-behavior-customer_A_video] quit
```

# Create a QoS policy named **customer\_A** for Customer A, and associate the classes with their respective behaviors in the QoS policy.

```

[PE_A] qos policy customer_A
[PE_A-qospolicy-customer_A] classifier customer_A_pc behavior customer_A_pc
[PE_A-qospolicy-customer_A] classifier customer_A_voice behavior customer_A_voice
[PE_A-qospolicy-customer_A] classifier customer_A_video behavior customer_A_video
[PE_A-qospolicy-customer_A] quit

Apply the QoS policy customer_A to the inbound direction of GigabitEthernet 1/0/1.
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] qos apply policy customer_A inbound
[PE_A-GigabitEthernet1/0/1] quit

Create traffic classes for matching Customer B's three traffic types.
[PE_A] traffic classifier customer_B_pc
[PE_A-classifier-customer_B_pc] if-match customer-vlan-id 15 to 25
[PE_A-classifier-customer_B_pc] quit
[PE_A] traffic classifier customer_B_voice
[PE_A-classifier-customer_B_voice] if-match customer-vlan-id 26 to 35
[PE_A-classifier-customer_B_voice] quit
[PE_A] traffic classifier customer_B_storage
[PE_A-classifier-customer_B_storage] if-match customer-vlan-id 36 to 40
[PE_A-classifier-customer_B_storage] quit

Configure SVLAN tagging 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-id 2001
[PE_A-behavior-customer_B_pc] remark dot1p 3
[PE_A-behavior-customer_B_pc] quit
[PE_A] traffic behavior customer_B_voice
[PE_A-behavior-customer_B_voice] nest top-most vlan-id 2002
[PE_A-behavior-customer_B_voice] remark dot1p 5
[PE_A-behavior-customer_B_voice] quit
[PE_A] traffic behavior customer_B_storage
[PE_A-behavior-customer_B_storage] nest top-most vlan-id 2003
[PE_A-behavior-customer_B_storage] remark dot1p 7
[PE_A-behavior-customer_B_storage] quit

Create a QoS policy named customer_B for Customer B, and associate the classes with their
respective behaviors in the QoS policy.
[PE_A] qos policy customer_B
[PE_A-qospolicy-customer_B] classifier customer_B_pc behavior customer_B_pc
[PE_A-qospolicy-customer_B] classifier customer_B_voice behavior customer_B_voice
[PE_A-qospolicy-customer_B] classifier customer_B_storage behavior
customer_B_storage
[PE_A-qospolicy-customer_B] quit

Apply the QoS policy customer_B to the inbound direction of GigabitEthernet 1/0/2.
[PE_A] interface gigabitethernet 1/0/2
[PE_A-GigabitEthernet1/0/2] qos apply policy customer_B inbound
[PE_A-GigabitEthernet1/0/2] quit

```

## Configuring PE B

1. Create 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 GigabitEthernet 1/0/1 (a customer-side port):

# Configure the port as a hybrid port, and remove it from VLAN 1.

```
[PE_B] interface gigabitethernet 1/0/1
[PE_B-GigabitEthernet1/0/1] port link-type hybrid
[PE_B-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

# Assign the port to SVLANs 2001 through 2003 as an untagged VLAN member.

```
[PE_B-GigabitEthernet1/0/1] port hybrid vlan 2001 to 2003 untagged
```

# Enable basic QinQ on the port.

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

# Configure the port to trust the 802.1p priority of frames.

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

3. Configure GigabitEthernet 1/0/2 (a customer-side port):

# Configure the port as a hybrid port, and remove it from VLAN 1.

```
[PE_B] interface gigabitethernet 1/0/2
[PE_B-GigabitEthernet1/0/2] port link-type hybrid
[PE_B-GigabitEthernet1/0/2] undo port hybrid vlan 1
```

# Assign the port to SVLANs 1001 through 1003 as an untagged VLAN member.

```
[PE_B-GigabitEthernet1/0/2] port hybrid vlan 1001 to 1003 untagged
```

# Enable basic QinQ on the port.

```
[PE_B-GigabitEthernet1/0/2] qinq enable
```

# Configure the port to trust the 802.1p priority of frames.

```
[PE_B-GigabitEthernet1/0/2] qos trust dot1p
[PE_B-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3 (the service provider-side port):

# Configure the port as a trunk port, and remove it from VLAN 1.

```
[PE_B] interface gigabitethernet 1/0/3
[PE_B-GigabitEthernet1/0/3] port link-type trunk
[PE_B-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

# Assign the port to SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
[PE_B-GigabitEthernet1/0/3] port trunk permit vlan 1001 to 1003 2001 to 2003
[PE_B-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-id 1001
[PE_B-behavior-customer_A_pc] remark dot1p 3
[PE_B-behavior-customer_A_pc] quit
[PE_B] traffic behavior customer_A_voice
[PE_B-behavior-customer_A_voice] nest top-most vlan-id 1002
[PE_B-behavior-customer_A_voice] remark dot1p 5
[PE_B-behavior-customer_A_voice] quit
[PE_B] traffic behavior customer_A_video
[PE_B-behavior-customer_A_video] nest top-most vlan-id 1003
[PE_B-behavior-customer_A_video] remark dot1p 7
[PE_B-behavior-customer_A_video] quit
Create a QoS policy named customer_A for Customer A, and associate the classes with their
respective behaviors in the QoS policy.
[PE_B] qos policy customer_A
[PE_B-qospolicy-customer_A] classifier customer_A_pc behavior customer_A_pc
[PE_B-qospolicy-customer_A] classifier customer_A_voice behavior customer_A_voice
[PE_B-qospolicy-customer_A] classifier customer_A_video behavior customer_A_video
[PE_B-qospolicy-customer_A] quit
Apply QoS policy customer_A to the inbound direction of GigabitEthernet 1/0/2.
[PE_B] interface gigabitethernet 1/0/2
[PE_B-GigabitEthernet1/0/2] qos apply policy customer_A inbound
[PE_B-GigabitEthernet1/0/2] quit
Create traffic classes for matching Customer B's three traffic types.
[PE_B] traffic classifier customer_B_pc
[PE_B-classifier-customer_B_pc] if-match customer-vlan-id 15 to 25
[PE_B-classifier-customer_B_pc] quit
[PE_B] traffic classifier customer_B_voice
[PE_B-classifier-customer_B_voice] if-match customer-vlan-id 26 to 35
[PE_B-classifier-customer_B_voice] quit
[PE_B] traffic classifier customer_B_storage
[PE_B-classifier-customer_B_storage] if-match customer-vlan-id 36 to 40
[PE_B-classifier-customer_B_storage] quit
Configure SVLAN tagging 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-id 2001
[PE_B-behavior-customer_B_pc] remark dot1p 3

```

```

[PE_B-behavior-customer_B_pc] quit
[PE_B] traffic behavior customer_B_voice
[PE_B-behavior-customer_B_voice] nest top-most vlan-id 2002
[PE_B-behavior-customer_B_voice] remark dot1p 5
[PE_B-behavior-customer_B_voice] quit
[PE_B] traffic behavior customer_B_storage
[PE_B-behavior-customer_B_storage] nest top-most vlan-id 2003
[PE_B-behavior-customer_B_storage] remark dot1p 7
[PE_B-behavior-customer_B_storage] quit

Create a QoS policy named customer_B for Customer B, and associate the classes with their
respective behaviors in the QoS policy.

[PE_B] qos policy customer_B
[PE_B-qospolicy-customer_B] classifier customer_B_pc behavior customer_B_pc
[PE_B-qospolicy-customer_B] classifier customer_B_voice behavior customer_B_voice
[PE_B-qospolicy-customer_B] classifier customer_B_storage behavior
customer_B_storage
[PE_B-qospolicy-customer_B] quit

Apply the QoS policy customer_B to the inbound direction of GigabitEthernet 1/0/1.

[PE_B] interface gigabitethernet 1/0/1
[PE_B-GigabitEthernet1/0/1] qos apply policy customer_B inbound
[PE_B-GigabitEthernet1/0/1] quit

```

## Configuring devices in the service provider network

Configure all ports on the path between PE A and PE B to meet the following requirements:

- Allow frames from VLANs 1001 through 1003 and VLANs 2001 through 2003 to pass through.
- Retain the VLAN tags of QinQ frames.

## Verifying the configuration

# Use the **display this** command to verify the configuration on each port, for example, on GigabitEthernet 1/0/1 of PE A.

```

[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1001 to 1003 untagged
 qinq enable
 qos apply policy customer_A inbound
#
Return
[PE_A-GigabitEthernet1/0/1] quit

```



# Use the **display qos policy interface** command to verify the QoS configuration on each port, for example, on GigabitEthernet 1/0/1 of PE A.

```
[PE_A] display qos policy interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
```

```
Direction: Inbound
```

```
Policy: customer_A
```

```
Classifier: customer_A_pc
```

```
Operator: AND
```

```
Rule(s) : If-match customer-vlan-id 10 to 20
```

```
Behavior: customer_A_pc
```

```
Nesting:
```

```
 Nest top-most vlan-id 1001
```

```
Marking:
```

```
 Remark dot1p COS 3
```

```
Classifier: customer_A_voice
```

```
Operator: AND
```

```
Rule(s) : If-match customer-vlan-id 21 to 30
```

```
Behavior: customer_A_voice
```

```
Nesting:
```

```
 Nest top-most vlan-id 1002
```

```
Marking:
```

```
 Remark dot1p COS 5
```

```
Classifier: customer_A_video
```

```
Operator: AND
```

```
Rule(s) : If-match customer-vlan-id 31 to 40
```

```
Behavior: customer_A_video
```

```
Nesting:
```

```
 Nest top-most vlan-id 1003
```

```
Marking:
```

```
 Remark dot1p COS 7
```

## Configuration files

- PE A:

```
#
vlan 1001 to 1003
#
vlan 2001 to 2003
#
traffic classifier customer_A_pc operator and
 if-match customer-vlan-id 10 to 20
traffic classifier customer_A_voice operator and
 if-match customer-vlan-id 21 to 30
traffic classifier customer_A_video operator and
 if-match customer-vlan-id 31 to 40
```

```

traffic classifier customer_B_pc operator and
 if-match customer-vlan-id 15 to 25
traffic classifier customer_B_voice operator and
 if-match customer-vlan-id 26 to 35
traffic classifier customer_B_storage operator and
 if-match customer-vlan-id 36 to 40
#
traffic behavior customer_A_pc
 nest top-most vlan-id 1001
 remark dot1p 3
traffic behavior customer_A_voice
 nest top-most vlan-id 1002
 remark dot1p 5
traffic behavior customer_A_video
 nest top-most vlan-id 1003
 remark dot1p 7
traffic behavior customer_B_pc
 nest top-most vlan-id 2001
 remark dot1p 3
traffic behavior customer_B_voice
 nest top-most vlan-id 2002
 remark dot1p 5
traffic behavior customer_B_storage
 nest top-most vlan-id 2003
 remark dot1p 7
#
qos policy customer_A
 classifier customer_A_pc behavior customer_A_pc
 classifier customer_A_voice behavior customer_A_voice
 classifier customer_A_video behavior customer_A_video
qos policy customer_B
 classifier customer_B_pc behavior customer_B_pc
 classifier customer_B_voice behavior customer_B_voice
 classifier customer_B_storage behavior customer_B_storage
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1001 to 1003 untagged
 qinq enable
 qos apply policy customer_A inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2001 to 2003 untagged

```

```

qinq enable
qos apply policy customer_B inbound
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 1001 to 1003 2001 to 2003
#
• PE B:
#
vlan 1001 to 1003
#
vlan 2001 to 2003
#
traffic classifier customer_A_pc operator and
if-match customer-vlan-id 10 to 20
traffic classifier customer_A_voice operator and
if-match customer-vlan-id 21 to 30
traffic classifier customer_A_video operator and
if-match customer-vlan-id 31 to 40
traffic classifier customer_B_pc operator and
if-match customer-vlan-id 15 to 25
traffic classifier customer_B_voice operator and
if-match customer-vlan-id 26 to 35
traffic classifier customer_B_storage operator and
if-match customer-vlan-id 36 to 40
#
traffic behavior customer_A_pc
nest top-most vlan-id 1001
remark dot1p 3
traffic behavior customer_A_voice
nest top-most vlan-id 1002
remark dot1p 5
traffic behavior customer_A_video
nest top-most vlan-id 1003
remark dot1p 7
traffic behavior customer_B_pc
nest top-most vlan-id 2001
remark dot1p 3
traffic behavior customer_B_voice
nest top-most vlan-id 2002
remark dot1p 5
traffic behavior customer_B_storage
nest top-most vlan-id 2003
remark dot1p 7
#
qos policy customer_A

```

```

classifier customer_A_pc behavior customer_A_pc
classifier customer_A_voice behavior customer_A_voice
classifier customer_A_video behavior customer_A_video
qos policy customer_B
classifier customer_B_pc behavior customer_B_pc
classifier customer_B_voice behavior customer_B_voice
classifier customer_B_storage behavior customer_B_storage
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 2001 to 2003 untagged
qinq enable
qos apply policy customer_B inbound
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 1001 to 1003 untagged
qinq enable
qos apply policy customer_A inbound
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 1001 to 1003 2001 to 2003
#

```

## Example: Configuring selective QinQ by binding CVLANs to SVLANs directly on customer-side ports

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

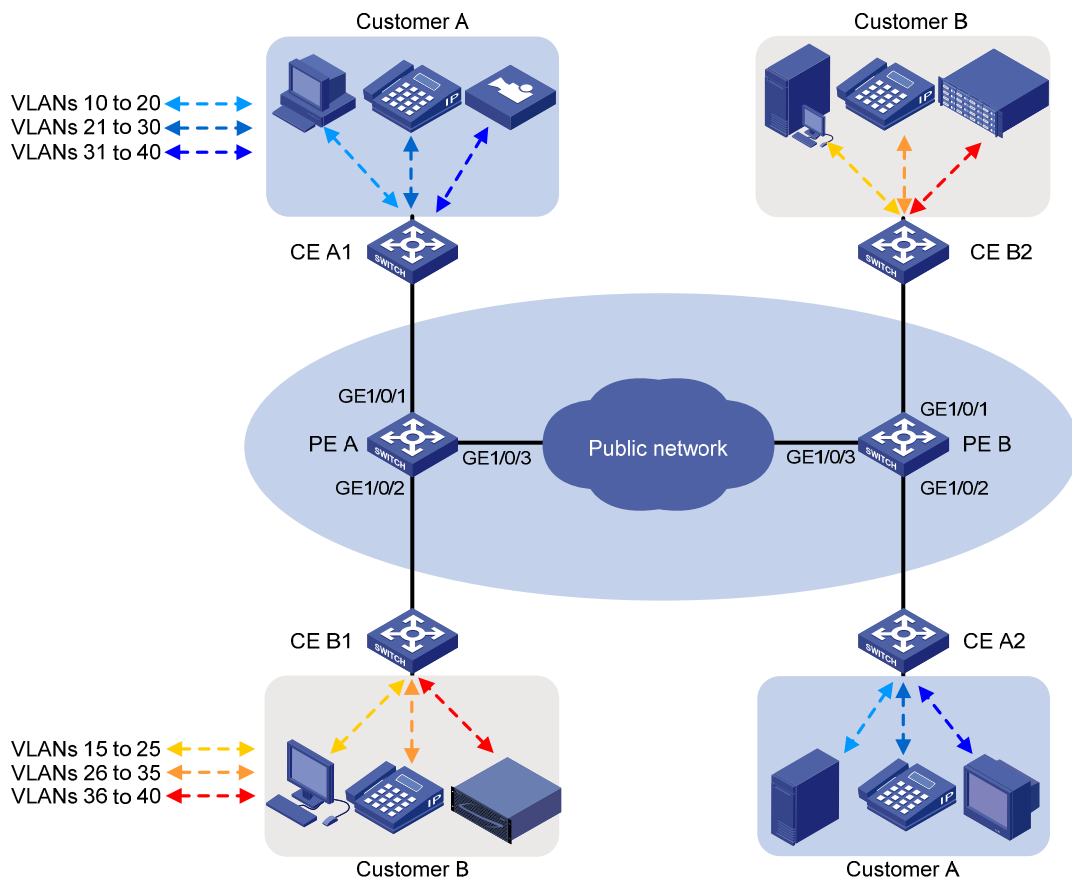
## Network requirements

As shown in [Figure 170](#), Customer A and Customer B each have two branches that require Layer 2 connectivity over the service provider network.

Both customers have three types of traffic and require different transmission priorities for the three types of traffic.

Configure selective QinQ on PE A and PE B to separate the traffic by customer and traffic type, and assign different 802.1p priority values to the traffic flows.

**Figure 170 Network diagram**



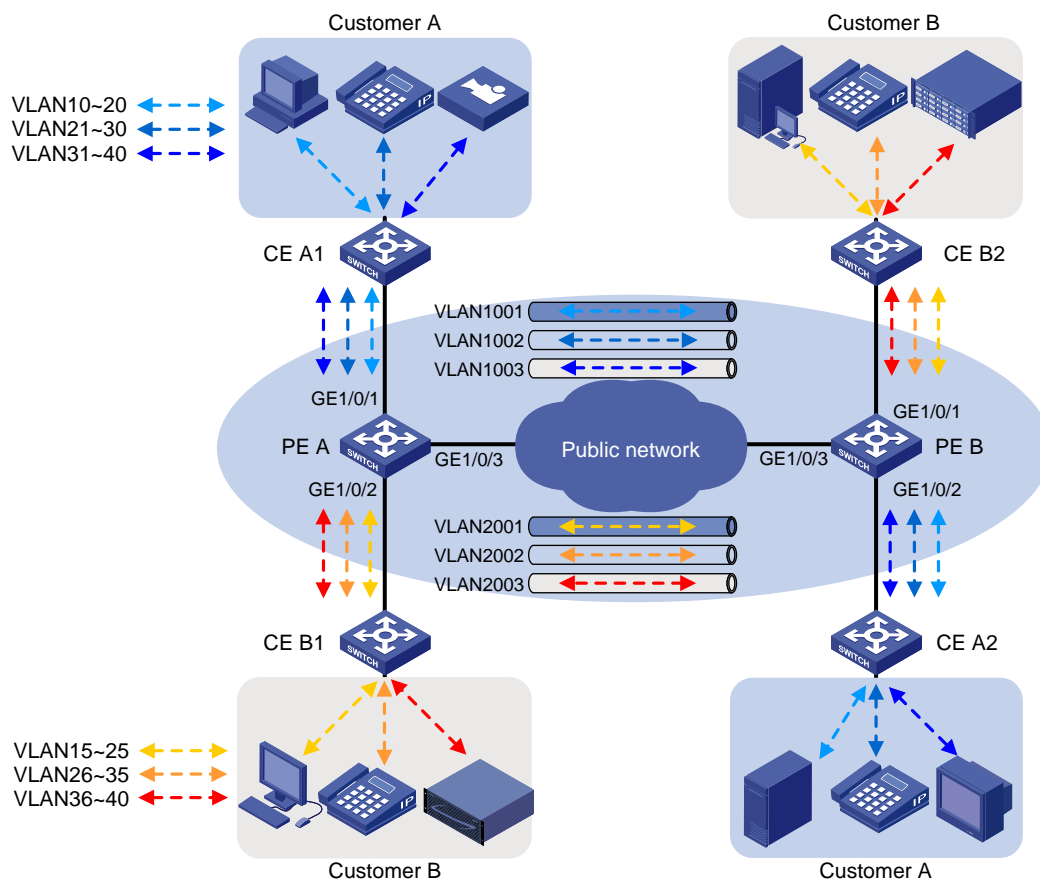
[Table 18](#) shows the VLAN assignment scheme. For each customer, the service provider assigns one SVLAN by traffic type. [Figure 171](#) shows the traffic transmission pattern after selective QinQ is configured.

**Table 18 VLAN assignment**

| Traffic type       | CVLANs   | SVLAN | Traffic priority |
|--------------------|----------|-------|------------------|
| <b>Customer A:</b> |          |       |                  |
| Video              | 31 to 40 | 1003  | High             |

| Traffic type       | CVLANs   | SVLAN | Traffic priority |
|--------------------|----------|-------|------------------|
| Voice              | 21 to 30 | 1002  | Medium           |
| Data               | 10 to 20 | 1001  | Low              |
| <b>Customer B:</b> |          |       |                  |
| Storage            | 36 to 40 | 2003  | High             |
| Voice              | 26 to 35 | 2002  | Medium           |
| Data               | 15 to 25 | 2001  | Low              |

Figure 171 Traffic pattern in the service provider network after selective QinQ is configured



## Requirements analysis

To run QinQ, you only need to configure selective QinQ on customer-side ports of PEs.

To implement selective QinQ, the customer-side ports must be hybrid ports, because they must support multiple SVLANs and must send traffic to the customer site with the SVLAN tag removed.

To send QinQ frames across the service provider network, you must configure all the ports on the forwarding path to meet the following requirements:

- Allow frames from VLAN 1000 and VLAN 2000 to pass through.
- Retain the VLAN tags of QinQ frames.

## Configuration restrictions and guidelines

When you configure selective QinQ, follow these restrictions and guidelines:

- You must enable basic QinQ before you can configure CVLAN to SVLAN bindings. If an incoming frame does not meet any bindings, the port adds the PVID tag to the frame as the SVLAN tag.
- On the HP 5500 EI switches, the 802.1p priority in the SVLAN tag added by a QinQ-enabled port depends on the priority trust mode on the port by default. 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.
- On the HP 5500 SI switches, a QinQ-enabled port encapsulates the port priority as the 802.1p priority in the SVLAN tag by default.
- A QinQ-enabled port cannot modify the CVLAN tag. To modify CVLAN IDs, configure CVLAN ID substitution on the service provider-side port. CVLAN ID substitution is available only on the HP 5500 EI switches.
- Increase the MTU to at least 1504 bytes for each port on the path of QinQ frames for forwarding QinQ frames.

## Configuration procedures

This example assumes that the CVLANs have been configured correctly on the CEs.

### 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 GigabitEthernet 1/0/1 (a customer-side port):

# Configure the port as a hybrid port, and remove it from VLAN 1.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] port link-type hybrid
[PE_A-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

# Assign the port to SVLANs 1001 through 1003 as an untagged VLAN member.

```
[PE_A-GigabitEthernet1/0/1] port hybrid vlan 1001 to 1003 untagged
```

# Enable basic QinQ on the port.

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

# Configure the port to tag frames from VLANs 10 through 20 with SVLAN 1001.

```
[PE_A-GigabitEthernet1/0/1] qinq vid 1001
```

```

[PE_A-GigabitEthernet1/0/1-vid-1001] raw-vlan-id inbound 10 to 20
[PE_A-GigabitEthernet1/0/1-vid-1001] quit
Configure the port to tag frames from VLANs 21 through 30 with SVLAN 1002.
[PE_A-GigabitEthernet1/0/1] qinq vid 1002
[PE_A-GigabitEthernet1/0/1-vid-1002] raw-vlan-id inbound 21 to 30
[PE_A-GigabitEthernet1/0/1-vid-1002] quit
Configure the port to tag frames from VLANs 31 through 40 with SVLAN 1003.
[PE_A-GigabitEthernet1/0/1] qinq vid 1003
[PE_A-GigabitEthernet1/0/1-vid-1003] raw-vlan-id inbound 31 to 40
[PE_A-GigabitEthernet1/0/1-vid-1003] quit
Configure the port to trust the 802.1p priority of frames.
[PE_A-GigabitEthernet1/0/1] qos trust dot1p
[PE_A-GigabitEthernet1/0/1] quit

```

### 3. Configure GigabitEthernet 1/0/2 (a customer-side port):

```

Configure the port as a hybrid port, and remove it from VLAN 1.
[PE_A] interface gigabitethernet 1/0/2
[PE_A-GigabitEthernet1/0/2] port link-type hybrid
[PE_A-GigabitEthernet1/0/2] undo port hybrid vlan 1
Assign the port to SVLANs 2001 through 2003 as an untagged VLAN member.
[PE_A-GigabitEthernet1/0/2] port hybrid vlan 2001 to 2003 untagged
Enable basic QinQ on the port.
[PE_A-GigabitEthernet1/0/2] qinq enable
Configure the port to tag frames from VLANs 15 through 25 with SVLAN 2001.
[PE_A-GigabitEthernet1/0/2] qinq vid 2001
[PE_A-GigabitEthernet1/0/2-vid-2001] raw-vlan-id inbound 15 to 25
[PE_A-GigabitEthernet1/0/2-vid-2001] quit
Configure the port to tag frames from VLANs 26 through 35 with SVLAN 2002.
[PE_A-GigabitEthernet1/0/2] qinq vid 2002
[PE_A-GigabitEthernet1/0/2-vid-2002] raw-vlan-id inbound 26 to 35
[PE_A-GigabitEthernet1/0/2-vid-2002] quit
Configure the port to tag frames from VLANs 36 through 40 with SVLAN 2003.
[PE_A-GigabitEthernet1/0/2] qinq vid 2003
[PE_A-GigabitEthernet1/0/2-vid-2003] raw-vlan-id inbound 36 to 40
[PE_A-GigabitEthernet1/0/2-vid-2003] quit
Configure the port to trust the 802.1p priority of frames.
[PE_A-GigabitEthernet1/0/2] qos trust dot1p
[PE_A-GigabitEthernet1/0/2] quit

```

### 4. Configure GigabitEthernet 1/0/3 (the service provider-side port):

```

Configure the port as a trunk port, and remove it from VLAN 1.
[PE_A] interface gigabitethernet 1/0/3
[PE_A-GigabitEthernet1/0/3] port link-type trunk
[PE_A-GigabitEthernet1/0/3] undo port trunk permit vlan 1
Assign the port to SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```



```
[PE_A-GigabitEthernet1/0/3] port trunk permit vlan 1001 to 1003 2001 to 2003
[PE_A-GigabitEthernet1/0/3] quit
```

5. Configure QoS policies for 802.1p priority re-mark:

# Create a class named **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 802.1p priority re-mark behaviors for Customer A's three traffic types.

```
[PE_A] traffic behavior customer_A_pc
[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] remark dot1p 5
[PE_A-behavior-customer_A_voice] quit
[PE_A] traffic behavior customer_A_video
[PE_A-behavior-customer_A_video] remark dot1p 7
[PE_A-behavior-customer_A_video] quit
```

# Create a QoS policy named **customer\_A** for Customer A, and associate the classes with their respective behaviors in the QoS policy.

```
[PE_A] qos policy customer_A
[PE_A-qospolicy-customer_A] classifier customer_A_pc behavior customer_A_pc
[PE_A-qospolicy-customer_A] classifier customer_A_voice behavior customer_A_voice
[PE_A-qospolicy-customer_A] classifier customer_A_video behavior customer_A_video
[PE_A-qospolicy-customer_A] quit
```

# Apply the QoS policy **customer\_A** to the inbound direction of GigabitEthernet 1/0/1.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] qos apply policy customer_A inbound
[PE_A-GigabitEthernet1/0/1] quit
```

# Create traffic classes for matching Customer B's three traffic types.

```
[PE_A] traffic classifier customer_B_pc
[PE_A-classifier-customer_B_pc] if-match customer-vlan-id 15 to 25
[PE_A-classifier-customer_B_pc] quit
[PE_A] traffic classifier customer_B_voice
[PE_A-classifier-customer_B_voice] if-match customer-vlan-id 26 to 35
[PE_A-classifier-customer_B_voice] quit
[PE_A] traffic classifier customer_B_storage
```

```
[PE_A-classifier-customer_B_storage] if-match customer-vlan-id 36 to 40
[PE_A-classifier-customer_B_storage] quit
```

# Configure 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] remark dot1p 3
[PE_A-behavior-customer_B_pc] quit
[PE_A] traffic behavior customer_B_voice
[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] remark dot1p 7
[PE_A-behavior-customer_B_storage] quit
```

# Create a QoS policy named **customer\_B** for Customer B, and associate the classes with their respective behaviors in the QoS policy.

```
[PE_A] qos policy customer_B
[PE_A-qospolicy-customer_B] classifier customer_B_pc behavior customer_B_pc
[PE_A-qospolicy-customer_B] classifier customer_B_voice behavior customer_B_voice
[PE_A-qospolicy-customer_B] classifier customer_B_storage behavior
customer_B_storage
[PE_A-qospolicy-customer_B] quit
```

# Apply the QoS policy **customer\_B** to the inbound direction of GigabitEthernet 1/0/2.

```
[PE_A] interface gigabitethernet 1/0/2
[PE_A-GigabitEthernet1/0/2] qos apply policy customer_B inbound
[PE_A-GigabitEthernet1/0/2] quit
```

## Configuring PE B

1. Create 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 GigabitEthernet 1/0/1 (a customer-side port):

# Configure the port as a hybrid port, and remove it from VLAN 1.

```
[PE_B] interface gigabitethernet 1/0/1
[PE_B-GigabitEthernet1/0/1] port link-type hybrid
[PE_B-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

# Assign the port to SVLANs 2001 through 2003 as an untagged VLAN member.

```
[PE_B-GigabitEthernet1/0/1] port hybrid vlan 2001 to 2003 untagged
```

# Enable basic QinQ on the port.

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

# Configure the port to tag frames from VLANs 15 through 25 with SVLAN 2001.

```
[PE_B-GigabitEthernet1/0/1] qinq vid 2001
[PE_B-GigabitEthernet1/0/1-vid-2001] raw-vlan-id inbound 15 to 25
[PE_B-GigabitEthernet1/0/1-vid-2001] quit
```

# Configure the port to tag frames from VLANs 26 through 35 with SVLAN 2002.

```
[PE_B-GigabitEthernet1/0/1] qinq vid 2002
```

```
[PE_B-GigabitEthernet1/0/1-vid-2002] raw-vlan-id inbound 26 to 35
[PE_B-GigabitEthernet1/0/1-vid-2002] quit
Configure the port to tag frames from VLANs 36 through 40 with SVLAN 2003.
[PE_B-GigabitEthernet1/0/1] qinq vid 2003
[PE_B-GigabitEthernet1/0/1-vid-2003] raw-vlan-id inbound 36 to 40
[PE_B-GigabitEthernet1/0/1-vid-2003] quit
Configure the port to trust the 802.1p priority of frames.
[PE_B-GigabitEthernet1/0/1] qos trust dot1p
[PE_B-GigabitEthernet1/0/1] quit
```

### 3. Configure GigabitEthernet 1/0/2 (a customer-side port):

```
Configure the port as a hybrid port, and remove it from VLAN 1.
[PE_B] interface gigabitethernet 1/0/2
[PE_B-GigabitEthernet1/0/2] port link-type hybrid
[PE_B-GigabitEthernet1/0/2] undo port hybrid vlan 1
Assign the port to SVLANs 1001 through 1003 as an untagged VLAN member.
[PE_B-GigabitEthernet1/0/2] port hybrid vlan 1001 to 1003 untagged
Enable basic QinQ on the port.
[PE_B-GigabitEthernet1/0/2] qinq enable
Configure the port to tag frames from VLANs 10 through 20 with SVLAN 1001.
[PE_B-GigabitEthernet1/0/2] qinq vid 1001
[PE_B-GigabitEthernet1/0/2-vid-1001] raw-vlan-id inbound 10 to 20
[PE_B-GigabitEthernet1/0/2-vid-1001] quit
Configure the port to tag frames from VLANs 21 through 30 with SVLAN 1002.
[PE_B-GigabitEthernet1/0/2] qinq vid 1002
[PE_B-GigabitEthernet1/0/2-vid-1002] raw-vlan-id inbound 21 to 30
[PE_B-GigabitEthernet1/0/2-vid-1002] quit
Configure the port to tag frames from VLANs 31 through 40 with SVLAN 1003.
[PE_B-GigabitEthernet1/0/2] qinq vid 1003
[PE_B-GigabitEthernet1/0/2-vid-1003] raw-vlan-id inbound 31 to 40
[PE_B-GigabitEthernet1/0/2-vid-1003] quit
Configure the port to trust the 802.1p priority of frames.
[PE_B-GigabitEthernet1/0/2] qos trust dot1p
[PE_B-GigabitEthernet1/0/2] quit
```

### 4. Configure GigabitEthernet 1/0/3 (the service provider-side port):

```
Configure the port as a trunk port, and remove it from VLAN 1.
[PE_B] interface gigabitethernet 1/0/3
[PE_B-GigabitEthernet1/0/3] port link-type trunk
[PE_B-GigabitEthernet1/0/3] undo port trunk permit vlan 1
Assign the port to SVLANs 1001 through 1003 and SVLANs 2001 through 2003.
[PE_B-GigabitEthernet1/0/3] port trunk permit vlan 1001 to 1003 2001 to 2003
[PE_B-GigabitEthernet1/0/3] quit
```

### 5. Configure QoS policies for 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 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] remark dot1p 3
[PE_B-behavior-customer_A_pc] quit
[PE_B] traffic behavior customer_A_voice
[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] remark dot1p 7
[PE_B-behavior-customer_A_video] quit

```

# Create a QoS policy named **customer\_A** for Customer A, and associate the classes with their respective behaviors in the QoS policy.

```

[PE_B] qos policy customer_A
[PE_B-qospolicy-customer_A] classifier customer_A_pc behavior customer_A_pc
[PE_B-qospolicy-customer_A] classifier customer_A_voice behavior customer_A_voice
[PE_B-qospolicy-customer_A] classifier customer_A_video behavior customer_A_video
[PE_B-qospolicy-customer_A] quit

```

# Apply the QoS policy **customer\_A** to the inbound direction of GigabitEthernet 1/0/2.

```

[PE_B] interface gigabitethernet 1/0/2
[PE_B-GigabitEthernet1/0/2] qos apply policy customer_A inbound
[PE_B-GigabitEthernet1/0/2] quit

```

# Create traffic classes for matching Customer B's three traffic types.

```

[PE_B] traffic classifier customer_B_pc
[PE_B-classifier-customer_B_pc] if-match customer-vlan-id 15 to 25
[PE_B-classifier-customer_B_pc] quit
[PE_B] traffic classifier customer_B_voice
[PE_B-classifier-customer_B_voice] if-match customer-vlan-id 26 to 35
[PE_B-classifier-customer_B_voice] quit
[PE_B] traffic classifier customer_B_storage
[PE_B-classifier-customer_B_storage] if-match customer-vlan-id 36 to 40
[PE_B-classifier-customer_B_storage] quit

```

# Configure 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] remark dot1p 3
[PE_B-behavior-customer_B_pc] quit
[PE_B] traffic behavior customer_B_voice
[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] remark dot1p 7
[PE_B-behavior-customer_B_storage] quit

Create a QoS policy named customer_B for Customer B, and associate the classes with their
respective behaviors in the QoS policy.

[PE_B] qos policy customer_B
[PE_B-qospolicy-customer_B] classifier customer_B_pc behavior customer_B_pc
[PE_B-qospolicy-customer_B] classifier customer_B_voice behavior customer_B_voice
[PE_B-qospolicy-customer_B] classifier customer_B_storage behavior
customer_B_storage
[PE_B-qospolicy-customer_B] quit

Apply the QoS policy customer_B to the inbound direction of GigabitEthernet 1/0/1.

[PE_B] interface gigabitethernet 1/0/1
[PE_B-GigabitEthernet1/0/1] qos apply policy customer_B inbound
[PE_B-GigabitEthernet1/0/1] quit

```

## Configuring devices in the service provider network

Configure all ports on the path between PE A and PE B to meet the following requirements:

- Allow frames from VLANs 1001 through 1003 and VLANs 2001 through 2003 to pass through.
- Retain the VLAN tags of QinQ frames.

## Verifying the configuration

# Use the **display this** command to verify the configuration on each port, for example, on GigabitEthernet 1/0/1 of PE A.

```

[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1001 to 1003 untagged
 qinq enable
 qinq vid 1001
 raw-vlan-id inbound 10 to 20
 qinq vid 1002
 raw-vlan-id inbound 21 to 30
 qinq vid 1003
 raw-vlan-id inbound 31 to 40
 qos apply policy customer_A inbound
#
Return
[PE_A-GigabitEthernet1/0/1] quit

```

# Use the **display qos policy interface** command to verify the QoS configuration on each port, for example, on GigabitEthernet 1/0/1 of PE A.

```
[PE_A] display qos policy interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
```

```
Direction: Inbound
```

```
Policy: customer_A
```

```
Classifier: customer_A_pc
```

```
Operator: AND
```

```
Rule(s) : If-match customer-vlan-id 10 to 20
```

```
Behavior: customer_A_pc
```

```
Marking:
```

```
Remark dot1p COS 3
```

```
Classifier: customer_A_voice
```

```
Operator: AND
```

```
Rule(s) : If-match customer-vlan-id 21 to 30
```

```
Behavior: customer_A_voice
```

```
Marking:
```

```
Remark dot1p COS 5
```

```
Classifier: customer_A_video
```

```
Operator: AND
```

```
Rule(s) : If-match customer-vlan-id 31 to 40
```

```
Behavior: customer_A_video
```

```
Marking:
```

```
Remark dot1p COS 7
```

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- 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
 remark dot1p 3
traffic behavior customer_A_voice
 remark dot1p 5
traffic behavior customer_A_video
 remark dot1p 7
traffic behavior customer_B_pc
 remark dot1p 3
traffic behavior customer_B_voice
 remark dot1p 5
traffic behavior customer_B_storage
 remark dot1p 7
#
qos policy customer_A
 classifier customer_A_pc behavior customer_A_pc
 classifier customer_A_voice behavior customer_A_voice
 classifier customer_A_video behavior customer_A_video
qos policy customer_B
 classifier customer_B_pc behavior customer_B_pc
 classifier customer_B_voice behavior customer_B_voice
 classifier customer_B_storage behavior customer_B_storage
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1001 to 1003 untagged
 qinq enable
qinq vid 1001
 raw-vlan-id inbound 10 to 20
qinq vid 1002
 raw-vlan-id inbound 21 to 30
qinq vid 1003
 raw-vlan-id inbound 31 to 40
qos apply policy customer_A inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2001 to 2003 untagged
 qinq enable
qinq vid 2001
 raw-vlan-id inbound 15 to 25
qinq vid 2002
 raw-vlan-id inbound 26 to 35

```

```

qinq vid 2003
 raw-vlan-id inbound 36 to 40
 qos apply policy customer_B inbound
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1001 to 1003 2001 to 2003
#

```

- PE B:

```

#
vlan 1001 to 1003
#
vlan 2001 to 2003
#
traffic classifier customer_A_pc operator and
 if-match customer-vlan-id 10 to 20
traffic classifier customer_A_voice operator and
 if-match customer-vlan-id 21 to 30
traffic classifier customer_A_video operator and
 if-match customer-vlan-id 31 to 40
traffic classifier customer_B_pc operator and
 if-match customer-vlan-id 15 to 25
traffic classifier customer_B_voice operator and
 if-match customer-vlan-id 26 to 35
traffic classifier customer_B_storage operator and
 if-match customer-vlan-id 36 to 40
#
traffic behavior customer_A_pc
 remark dot1p 3
traffic behavior customer_A_voice
 remark dot1p 5
traffic behavior customer_A_video
 remark dot1p 7
traffic behavior customer_B_pc
 remark dot1p 3
traffic behavior customer_B_voice
 remark dot1p 5
traffic behavior customer_B_storage
 remark dot1p 7
#
qos policy customer_A
 classifier customer_A_pc behavior customer_A_pc
 classifier customer_A_voice behavior customer_A_voice
 classifier customer_A_video behavior customer_A_video
qos policy customer_B
 classifier customer_B_pc behavior customer_B_pc

```



```

classifier customer_B_voice behavior customer_B_voice
classifier customer_B_storage behavior customer_B_storage
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 2001 to 2003 untagged
qinq enable
qinq vid 2001
raw-vlan-id inbound 15 to 25
qinq vid 2002
raw-vlan-id inbound 26 to 35
qinq vid 2003
raw-vlan-id inbound 36 to 40
qos apply policy customer_B inbound
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 1001 to 1003 untagged
qinq enable
qinq vid 1001
raw-vlan-id inbound 10 to 20
qinq vid 1002
raw-vlan-id inbound 21 to 30
qinq vid 1003
raw-vlan-id inbound 31 to 40
qos apply policy customer_A inbound
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 1001 to 1003 2001 to 2003
#

```

# Example: Changing the CVLAN TPID and SVLAN TPID (HP 5500 EI)

## Applicable product matrix

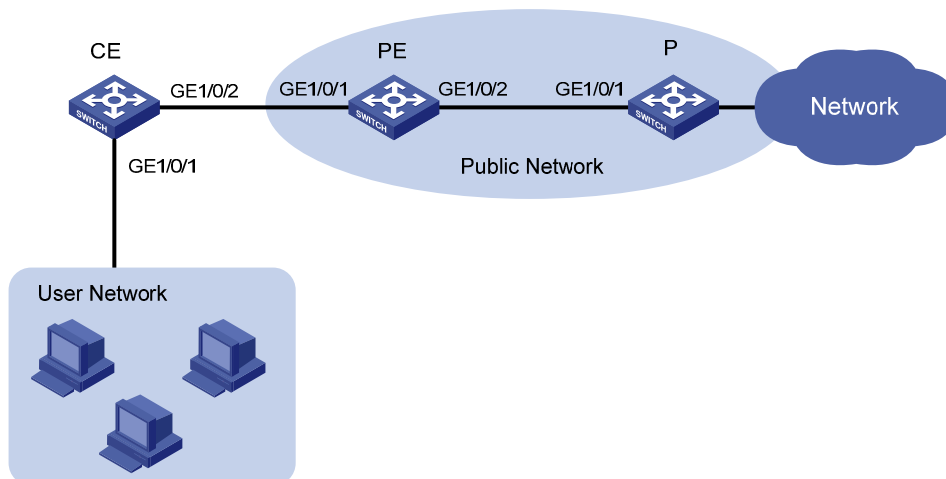
| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |

## Network requirements

Basic QinQ is enabled on GigabitEthernet 1/0/1 of the PE in [Figure 172](#). The TPID in the 802.1Q-tagged frames from the CE is 0x8200, and 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 172 Network diagram**



## Requirements analysis

The switch supports one global CVLAN PVID for all QinQ-enabled ports. On a port with basic QinQ or customer-side QinQ (**qinq enable downlink**) enabled, the switch identifies VLAN tagged frames based on the global CVLAN TPID. However, the switch does not change the TPID in CVLAN tags. An incoming frame is handled as an untagged frame if its TPID is different from the global CVLAN TPID.

If you are implementing selective QinQ, you must make sure the CVLAN TPID on the switch is the same as the VLAN TPID on the customer device. TPID mismatch can result in SVLAN assignment mistake. If you

are implementing basic QinQ, you do not need to change the CVLAN TPID because CVLAN TPID mismatch does not affect SVLAN assignment.

For the PE in this example to identify CVLAN-tagged frames correctly on GigabitEthernet 1/0/1, you must change the global CVLAN TPID to 0x8200.

The switch supports only one SVLAN PVID for all ports. 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 the PE.

## Configuration restrictions and guidelines

TPID identifies a frame as an 802.1Q tagged frame. By default, the switch sets the TPID in 802.1Q VLAN tags to 0x8100 and identifies frames that carry 0x8100 as tagged. This value might differ by vendor. 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.

## 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. Set the CVLAN TPID to 0x8200.

```
[PE] qinq ethernet-type customer-tag 8200
```

3. Set the SVLAN TPID to 0x9100.

```
[PE] qinq ethernet-type service-tag 9100
```

4. Configure GigabitEthernet 1/0/1 (the customer-side port):

# Configure the port as a hybrid port, set its PVID to 1000, and remove it from VLAN 1.

```
[PE] interface gigabitEthernet 1/0/1
[PE-GigabitEthernet1/0/1] port link-type hybrid
[PE-GigabitEthernet1/0/1] port hybrid pvid vlan 1000
[PE-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

# Assign the port to VLAN 1000 as an untagged VLAN member.

```
[PE-GigabitEthernet1/0/1] port hybrid vlan 1000 untagged
```

# Enable basic QinQ on GigabitEthernet 1/0/1.

```
[PE-GigabitEthernet1/0/1] qinq enable
[PE-GigabitEthernet1/0/1] quit
```

5. Configure GigabitEthernet 1/0/2 (the service-provider-side port):

# Configure the port as a trunk port, assign it to VLAN 1000, and remove it from VLAN 1.

```
[PE] interface gigabitEthernet 1/0/2
```

```
[PE-GigabitEthernet1/0/2] port link-type trunk
[PE-GigabitEthernet1/0/2] port trunk permit vlan 1000
[PE-GigabitEthernet1/0/2] undo port trunk permit vlan 1
```

## Verifying the configuration

# Use the **display current-configuration | include qinq ethernet-type** command to verify the CVLAN and SVLAN TPID settings.

```
[PE] display current-configuration | include qinq ethernet-type
qinq ethernet-type service-tag 9100
qinq ethernet-type customer-tag 8200
```

---

### NOTE:

There are no commands to display the initial settings. If the default TPID is 0x8100 (the initial setting), the **display current-configuration** command do not display the TPID setting.

---

## Configuration files

```
#
qinq ethernet-type service-tag 9100
qinq ethernet-type customer-tag 8200
#
vlan 1000
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 1000 untagged
port hybrid pvid vlan 1000
qinq enable
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 1000
#
```

# Example: Changing the TPID (HP 5500 SI)

## Applicable product matrix

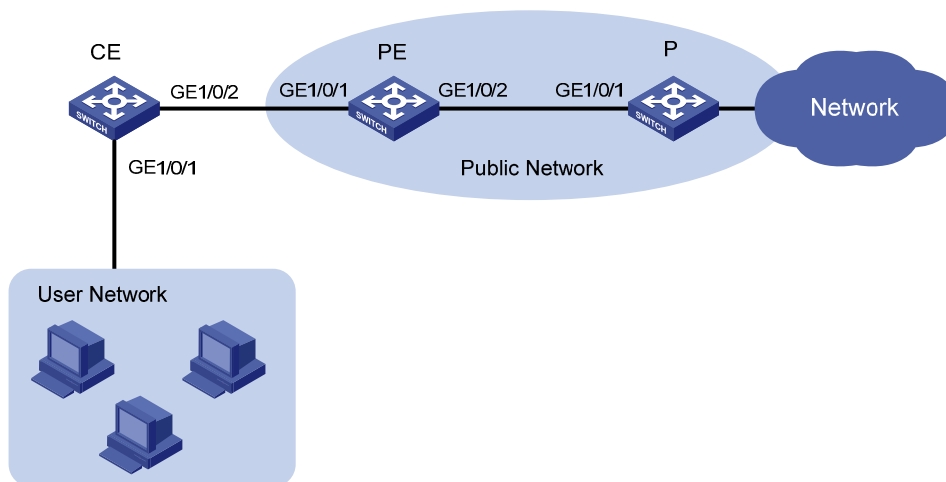
| Product series | Software version |
|----------------|------------------|
| HP 5500 SI     | Release 2220     |

## Network requirements

Basic QinQ is enabled on GigabitEthernet 1/0/1 of the PE in [Figure 173](#). The TPID in the 802.1Q-tagged frames from the CE and the P device is 0x9100.

Change the TPID on the PE to be compatible with the CE and the P device.

**Figure 173 Network diagram**



## Requirements analysis

The switch supports only one TPID for all ports.

On a QinQ-enabled port, the switch identifies VLAN tagged frames based on the 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 specified TPID.

If you are implementing selective QinQ, you must make sure the 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 basic QinQ, CVLAN TPID mismatch does not affect SVLAN assignment.

A service providers-side port uses the 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 TPID to 0x9100 on the PE.

## Configuration restrictions and guidelines

TPID identifies a frame as an 802.1Q tagged frame. By default, the switch sets the TPID in 802.1Q VLAN tags to 0x8100 and identifies frames that carry 0x8100 as tagged. This value might differ by vendor. 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.

## 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. Set the TPID to 0x9100.

```
[PE] qinq ethernet-type 9100
```

3. Configure GigabitEthernet 1/0/1 (the customer-side port):

# Configure the port as a hybrid port, set its PVID to 1000, and remove it from VLAN 1.

```
[PE] interface gigabitethernet 1/0/1
[PE-GigabitEthernet1/0/1] port link-type hybrid
[PE-GigabitEthernet1/0/1] port hybrid pvid vlan 1000
[PE-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

# Assign the port to VLAN 1000 as an untagged VLAN member.

```
[PE-GigabitEthernet1/0/1] port hybrid vlan 1000 untagged
```

# Enable basic QinQ on GigabitEthernet 1/0/1.

```
[PE-GigabitEthernet1/0/1] qinq enable
[PE-GigabitEthernet1/0/1] quit
```

4. Configure GigabitEthernet 1/0/2 (the service-provider-side port):

# Configure the port as a trunk port, assign it to VLAN 1000, and remove it from VLAN 1.

```
[PE] interface gigabitethernet 1/0/2
[PE-GigabitEthernet1/0/2] port link-type trunk
[PE-GigabitEthernet1/0/2] port trunk permit vlan 1000
[PE-GigabitEthernet1/0/2] undo port trunk permit vlan 1
```

## Verifying the configuration

# Use the **display current-configuration | include qinq ethernet-type** command to verify the TPID settings.

```
[PE] display current-configuration | include qinq ethernet-type
qinq ethernet-type 9100
```

---

**NOTE:**

There are no commands to display the initial settings. If the default TPID is 0x8100 (the initial setting), the **display current-configuration** command do not display the TPID setting.

---

## Configuration files

```
#
qinq ethernet-type 9100
#
vlan 1000
#
interface 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 GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1000
#
```

# Traffic policing configuration examples

This chapter provides examples for configuring traffic policing and aggregate CAR to control network traffic.

## Example: Policing traffic by IP address and protocol

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

### Network requirements

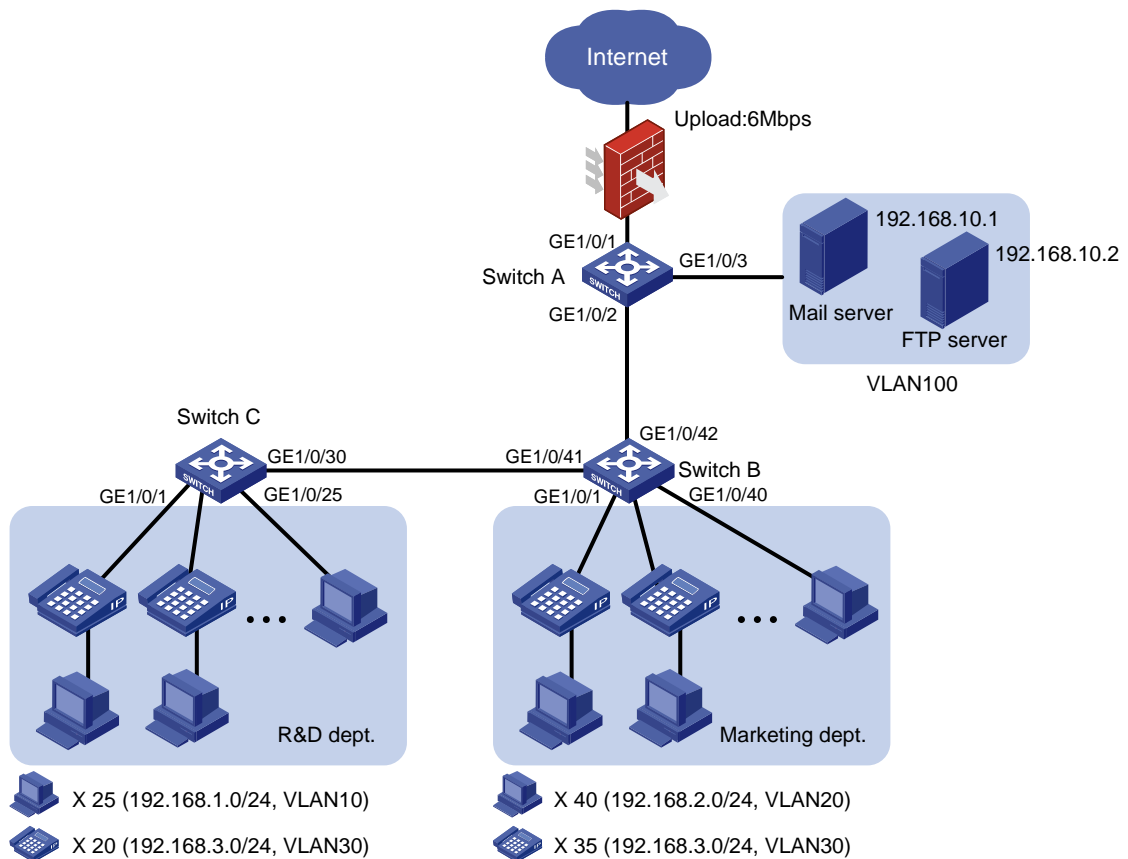
As shown in [Figure 174](#), a company uses a dedicated line to access the Internet, with an uplink bandwidth of 6 Mbps. All end devices use the firewall as the gateway.

Configure traffic policing to classify and rate limit the upstream traffic as follows:

- **HTTP traffic**—Rate limit HTTP traffic to a total of 3 Mbps. 1 Mbps is for the 25 hosts in the R & D department, and each host is limited to a maximum of 128 kbps. 2 Mbps is for the 40 hosts in the Marketing department, and each host is limited to a maximum of 256 kbps.
- **VoIP traffic**—Rate limit VoIP traffic to 640 kbps for the 55 IP phones in the two departments. An IP phone requires 32 kbps when in conversation. 640 kbps supports 20 IP phones that are in calls simultaneously. To accommodate more IP phones, a peak rate of 800 kbps is allowed.
- **Email traffic**—A mail server forwards emails for all clients to the external network. Rate limit email traffic to 512 kbps.
- **FTP traffic**—An FTP server provides data services for the branches through the external network. Rate limit email traffic to 1 Mbps.



Figure 174 Network diagram



## Configuration restrictions and guidelines

In a traffic behavior, the traffic policing action cannot be configured together with a priority marking action. Otherwise, a QoS policy that references such a behavior cannot be applied correctly. Priority marking actions include local precedence, drop precedence, 802.1p priority, DSCP, and IP precedence marking.

## Configuration procedures

### Configuring Switch A

1. Configure VLAN attributes for the interfaces:

# Configure GigabitEthernet 1/0/1 as a trunk port.

```
<SwitchA> system-view
```

```
[SwitchA] interface gigabitethernet 1/0/1
```

```
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
```

# Assign the port to VLAN 10, VLAN 20, VLAN 30, and VLAN 100.

```
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 10 20 30 100
```

```

Remove the port from VLAN 1.
[SwitchA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchA-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2 as a trunk port.
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk

Assign the port to VLAN 10, VLAN 20, and VLAN 30.
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 10 20 30

Remove the port from VLAN 1.
[SwitchA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[SwitchA-GigabitEthernet1/0/2] quit

Configure GigabitEthernet 1/0/3 as an access port.
<SwitchA> system-view
[SwitchA] interface gigabitethernet 1/0/3

Assign the port to VLAN 100.
[SwitchA-GigabitEthernet1/0/3] port access vlan 100
[SwitchA-GigabitEthernet1/0/3] quit

```

## 2. Configure traffic classes and behaviors for HTTP traffic:

```

Create advanced IPv4 ACL 3000 to match the HTTP traffic from the R & D department.
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule permit tcp destination-port eq 80 source 192.168.1.0
0.0.0.255
[SwitchA-acl-adv-3000] quit

Create a class named rd_http, and use advanced IPv4 ACL 3000 as the match criterion.
[SwitchA] traffic classifier rd_http
[SwitchA-classifier-rd_http] if-match acl 3000
[SwitchA-classifier-rd_http] quit

Create a behavior named rd_http, and configure traffic policing (1024 kbps CIR and 6225
bytes CBS).
[SwitchA] traffic behavior rd_http
[SwitchA-behavior-rd_http] car cir 1024 cbs 6225
[SwitchA-behavior-rd_http] quit

Create advanced IPv4 ACL 3001 to match the HTTP traffic from the Marketing department.
[SwitchA] acl number 3001
[SwitchA-acl-adv-3001] rule permit tcp destination-port eq 80 source 192.168.2.0
0.0.0.255
[SwitchA-acl-adv-3001] quit

Create a class named mkt_http, and use advanced IPv4 ACL 3001 as the match criterion.
[SwitchA] traffic classifier mkt_http
[SwitchA-classifier-mkt_http] if-match acl 3001
[SwitchA-classifier-mkt_http] quit

Create a behavior named mkt_http, and configure traffic policing (2048 kbps CIR and 13108
bytes CBS).

```

```
[SwitchA] traffic behavior mkt_http
[SwitchA-behavior-mkt_http] car cir 2048 cbs 13108
[SwitchA-behavior-mkt_http] quit
```

**3. Configure traffic classes and behaviors for VoIP traffic:**

# Create basic IPv4 ACL 2000 to match the VoIP traffic.

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 192.168.3.0 0.0.0.255
[SwitchA-acl-basic-2000] quit
```

# Create a class named **ip\_voip**, and use basic IPv4 ACL 2000 as the match criterion.

```
[SwitchA] traffic classifier ip_voip
[SwitchA-classifier-ip_voip] if-match acl 2000
[SwitchA-classifier-ip_voip] quit
```

# Create a behavior named **ip\_voip**, and configure traffic policing (640 kbps CIR, 4096 bytes CBS, 1024 bytes EBS, and 800 kbps PIR).

```
[SwitchA] traffic behavior ip_voip
[SwitchA-behavior-ip_voip] car cir 640 cbs 4096 ebs 1024 pir 800
[SwitchA-behavior-ip_voip] quit
```

**4. Configure traffic classes and behaviors for email traffic:**

# Create advanced IPv4 ACL 3002 to match the email traffic.

```
[SwitchA] acl number 3002
[SwitchA-acl-adv-3002] rule permit tcp destination-port eq smtp source 192.168.10.1
0.0.0.0
[SwitchA-acl-adv-3002] quit
```

# Create a class named **email**, and use advanced IPv4 ACL 3002 as the match criterion.

```
[SwitchA] traffic classifier email
[SwitchA-classifier-email] if-match acl 3002
[SwitchA-classifier-email] quit
```

# Create a behavior named **email**, and configure traffic policing (512 kbps CIR and 3277 bytes CBS).

```
[SwitchA] traffic behavior email
[SwitchA-behavior-email] car cir 512 cbs 3277
[SwitchA-behavior-email] quit
```

**5. Configure traffic classes and behaviors for FTP traffic:**

# Create basic IPv4 ACL 2001 to match the FTP traffic.

```
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 192.168.10.2 0.0.0.0
[SwitchA-acl-basic-2001] quit
```

# Create a class named **ftp**, and use advanced IPv4 ACL 2001 as the match criterion.

```
[SwitchA] traffic classifier ftp
[SwitchA-classifier-ftp] if-match acl 2001
[SwitchA-classifier-ftp] quit
```

# Create a behavior named **ftp**, and configure traffic policing (1024 kbps CIR and 6554 bytes CBS).

```
[SwitchA] traffic behavior ftp
[SwitchA-behavior-ftp] car cir 1024 cbs 6554
[SwitchA-behavior-ftp] quit
```

## 6. Configure QoS policies and apply them to interfaces:

# Create a QoS policy named **http&voice**.

```
[SwitchA] qos policy http&voice
```

# Associate the classes **rd\_http**, **mkt\_http**, and **ip\_voip** with the behaviors **rd\_http**, **mkt\_http**, and **ip\_voip** in **http&voice**, respectively.

```
[SwitchA-qospolicy-http&voice] classifier rd_http behavior rd_http
[SwitchA-qospolicy-http&voice] classifier mkt_http behavior mkt_http
[SwitchA-qospolicy-http&voice] classifier ip_voip behavior ip_voip
[SwitchA-qospolicy-http&voice] quit
```

# Apply the QoS policy **http&voice** to the inbound direction of GigabitEthernet 1/0/2.

```
[SwitchA] interface GigabitEthernet1/0/2
[SwitchA-GigabitEthernet1/0/2] qos apply policy http&voice inbound
[SwitchA-GigabitEthernet1/0/2] quit
```

# Create a QoS policy named **email&ftp**.

```
[SwitchA] qos policy email&ftp
```

# Associate the classes **email** and **ftp** with the behaviors **email** and **ftp** in **email&ftp**, respectively.

```
[SwitchA-qospolicy-email&ftp] classifier email behavior email
[SwitchA-qospolicy-email&ftp] classifier ftp behavior ftp
[SwitchA-qospolicy-email&ftp] quit
```

# Apply the QoS policy **email&ftp** to the inbound direction of GigabitEthernet 1/0/3.

```
[SwitchA] interface GigabitEthernet1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-mode bridge
[SwitchA-GigabitEthernet1/0/3] qos apply policy email&ftp inbound
```

## Configuring Switch B

In this example, the IP phones support sending VLAN-tagged voice packets. For information about how IP phones obtain VLAN information, see the configuration guide for the switch.

If the switch is configured with the auto-mode voice VLAN function, the interfaces connecting to IP phones do not need to be assigned to VLAN 30.

### 1. Configure interfaces and VLANs:

# Create port group 1.

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

# Add all interfaces that connect to hosts and IP phones to port group 1.

```
[SwitchB-port-group-manual-1] group-member GigabitEthernet 1/0/1 to GigabitEthernet 1/0/40
```

# Configure the interfaces in port group 1 as trunk ports.

```
[SwitchB-port-group-manual-1] port link-type trunk
```

# Configure the PVID of these interfaces as VLAN 20.

```
[SwitchB-port-group-manual-1] port trunk pvid vlan 20
```

```

Assign these interfaces to VLAN 20 and VLAN 30, and remove these interfaces from VLAN 1.
[SwitchB-port-group-manual-1] port trunk permit vlan 20 30
[SwitchB-port-group-manual-1] undo port trunk permit vlan 1
[SwitchB-port-group-manual-1] quit

Configure GigabitEthernet 1/0/41 as a trunk port.
[SwitchB] interface gigabitethernet 1/0/41
[SwitchB-GigabitEthernet1/0/41] port link-type trunk

Assign GigabitEthernet 1/0/41 to VLAN 10 and VLAN 30, and remove it from VLAN 1.
[SwitchB-GigabitEthernet1/0/41] port trunk permit vlan 10 30
[SwitchB-GigabitEthernet1/0/41] undo port trunk permit vlan 1
[SwitchB-GigabitEthernet1/0/41] quit

Configure GigabitEthernet 1/0/42 as a trunk port.
[SwitchB] interface gigabitethernet 1/0/42
[SwitchB-GigabitEthernet1/0/42] port link-type trunk

Assign it to VLAN 10, VLAN 20, and VLAN 30, and remove it from VLAN 1.
[SwitchB-GigabitEthernet1/0/42] port trunk permit vlan 10 20 30
[SwitchB-GigabitEthernet1/0/42] undo port trunk permit vlan 1
[SwitchB-GigabitEthernet1/0/42] quit

```

## 2. Configure traffic policing:

```

Create advanced IPv4 ACL 3000 to match the HTTP traffic from the Marketing department.
[SwitchB] acl number 3000
[SwitchB-acl-adv-3000] rule permit tcp destination-port eq 80 source 192.168.2.0
0.0.0.255
[SwitchB-acl-adv-3000] quit

Create a class named mkt, and use advanced IPv4 ACL 3000 as the match criterion.
[SwitchB] traffic classifier mkt
[SwitchB-classifier-mkt] if-match acl 3000
[SwitchB-classifier-mkt] quit

Create a behavior named mkt, and configure traffic policing: CIR 256 kbps and CBS 1638
bytes.
[SwitchB] traffic behavior mkt
[SwitchB-behavior-mkt] car cir 256 cbs 1638
[SwitchB-behavior-mkt] quit

Create a QoS policy named mkt, and associate the class mkt with the behavior mkt in mkt.
[SwitchB] qos policy mkt
[SwitchB-qospolicy-mkt] classifier mkt behavior mkt

Apply the QoS policy mkt to the inbound direction of port group 1.
[SwitchB] port-group manual 1
[SwitchB-port-group-manual-1] qos apply policy mkt inbound

```

## Configuring Switch C

### 1. Configure interfaces and VLANs:

```

Create port group 1.

```

```

<SwitchC> system-view
[SwitchC] port-group manual 1
Add all interfaces that connect to hosts and IP phones to port group 1.
[SwitchC-port-group-manual-1] group-member GigabitEthernet 1/0/1 to GigabitEthernet
1/0/25
Configure the interfaces in port group 1 as trunk ports.
[SwitchC-port-group-manual-1] port link-type trunk
Configure the PVID of these interfaces as VLAN 10.
[SwitchC-port-group-manual-1] port trunk pvid vlan 10
Assign these interfaces to VLAN 10 and VLAN 30, and remove these interfaces from VLAN 1.
[SwitchC-port-group-manual-1] port trunk permit vlan 10 30
[SwitchC-port-group-manual-1] undo port trunk permit vlan 1
[SwitchC-port-group-manual-1] quit
Configure GigabitEthernet 1/0/30 as a trunk port.
[SwitchC] interface gigabitethernet 1/0/30
[SwitchC-GigabitEthernet1/0/30] port link-type trunk
[SwitchC-GigabitEthernet1/0/30] port trunk permit vlan 10 30
Assign it to VLAN 10 and VLAN 30, and remove it from VLAN 1.
[SwitchC-GigabitEthernet1/0/30] undo port trunk permit vlan 1
[SwitchC-GigabitEthernet1/0/30] quit

```

## 2. Configure traffic policing:

# Create advanced IPv4 ACL 3000 to match the HTTP traffic from the R&D department.

```

[SwitchC] acl number 3000
[SwitchC-acl-adv-3000] rule permit tcp destination-port eq 80 source 192.168.1.0
0.0.0.255
[SwitchC-acl-adv-3000] quit

```

# Create a class named **rd**, and use advanced IPv4 ACL 3000 as the match criterion.

```

[SwitchC] traffic classifier rd
[SwitchC-classifier-rd] if-match acl 3000
[SwitchC-classifier-rd] quit

```

# Create a behavior named **rd**, and configure traffic policing: CIR 128 kbps and CBS 820 bytes.

```

[SwitchC] traffic behavior rd
[SwitchC-behavior-rd] car cir 128 cbs 820
[SwitchC-behavior-rd] quit

```

# Create a QoS policy named **rd**, and associate the class **rd** with the behavior **rd** in the QoS policy **rd**.

```

[SwitchC] qos policy rd
[SwitchC-qospolicy-rd] classifier rd behavior rd

```

# Apply the QoS policy **rd** to the inbound direction of port group 1.

```

[SwitchC] port-group manual 1
[SwitchC-port-group-manual-1] qos apply policy rd inbound

```

# Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```
#
acl number 2000
 rule 0 permit source 192.168.3.0 0.0.0.255
acl number 2001
 rule 0 permit source 192.168.10.2 0
#
acl number 3000
 rule 0 permit tcp source 192.168.1.0 0.0.0.255 destination-port eq www
acl number 3001
 rule 0 permit tcp source 192.168.2.0 0.0.0.255 destination-port eq www
acl number 3002
 rule 0 permit tcp source 192.168.10.1 0 destination-port eq smtp
#
traffic classifier email operator and
 if-match acl 3002
traffic classifier ip_voip operator and
 if-match acl 2000
traffic classifier ftp operator and
 if-match acl 2001
traffic classifier rd_http operator and
 if-match acl 3000
traffic classifier mkt_http operator and
 if-match acl 3001
#
traffic behavior email
 car cir 512 cbs 3277 ebs 512 green pass red discard yellow pass
traffic behavior ip_voip
 car cir 640 cbs 4096 ebs 1024 pir 800 green pass red discard yellow pass
traffic behavior ftp
 car cir 1024 cbs 6554 ebs 512 green pass red discard yellow pass
traffic behavior rd_http
 car cir 1024 cbs 6554 ebs 512 green pass red discard yellow pass
traffic behavior mkt_http
 car cir 2048 cbs 13108 ebs 512 green pass red discard yellow pass
#
qos policy email&ftp
 classifier email behavior email
 classifier ftp behavior ftp
qos policy http&voice
 classifier rd_http behavior rd_http
 classifier mkt_http behavior mkt_http
 classifier ip_voip behavior ip_voip
#
```

```

interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30
 qos apply policy http&voice inbound
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
 qos apply policy email&ftp inbound

```

- **Switch B:**

```

#
acl number 3000
 rule 0 permit tcp source 192.168.2.0 0.0.0.255 destination-port eq www
#
traffic classifier mkt operator and
 if-match acl 3000
#
traffic behavior mkt
 car cir 256 cbs 1638 ebs 512 green pass red discard yellow pass
#
qos policy mkt
 classifier mkt behavior mkt
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
 port trunk pvid vlan 20
 qos apply policy mkt inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
 port trunk pvid vlan 20
 qos apply policy mkt inbound
#
interface GigabitEthernet1/0/3

```



```

port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 20 30
port trunk pvid vlan 20
qos apply policy mkt inbound
...
#
interface GigabitEthernet1/0/41
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 30
qos apply policy mkt inbound
#
interface GigabitEthernet1/0/42
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30
qos apply policy mkt inbound

```

- Switch C:

```

#
acl number 3000
rule 0 permit tcp source 192.168.1.0 0.0.0.255 destination-port eq www
#
traffic classifier rd operator and
if-match acl 3000
#
traffic behavior rd
car cir 128 cbs 820 ebs 512 green pass red discard yellow pass
#
qos policy rd
classifier rd behavior rd
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 30
port trunk pvid vlan 10
qos apply policy rd inbound
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 30

```

```
port trunk pvid vlan 10
qos apply policy rd inbound
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 30
port trunk pvid vlan 10
qos apply policy rd inbound
...
#
interface GigabitEthernet1/0/30
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 30
```

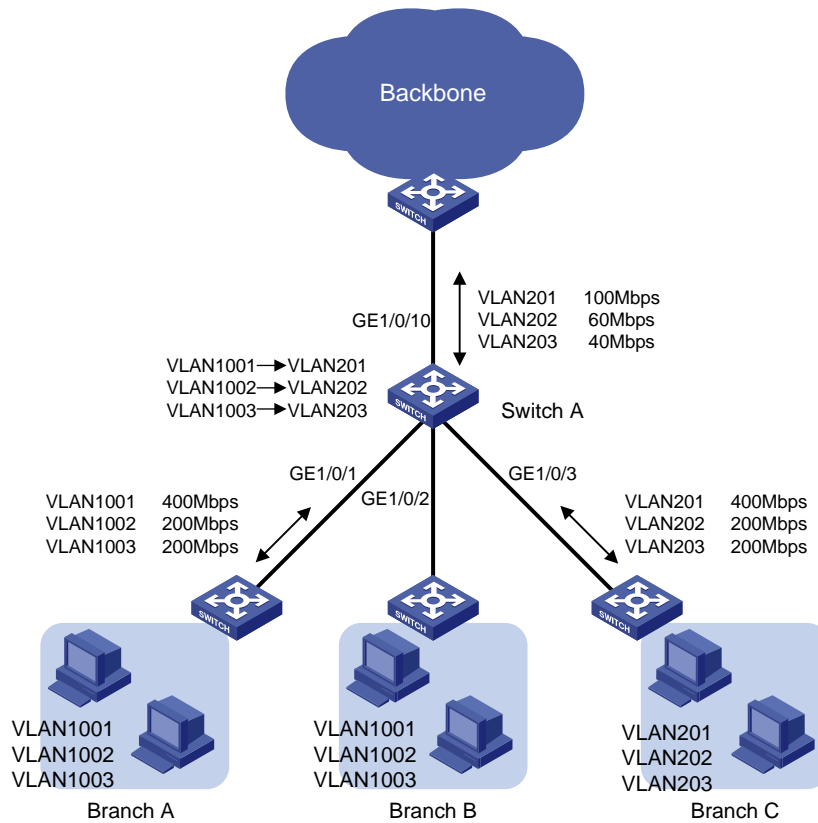
## Example: Allocating bandwidth based on VLANs

### Applicable product matrix

| <b>Product series</b> | <b>Software version</b> |
|-----------------------|-------------------------|
| HP 5500 EI            | Release 2220            |

# Network requirements

Figure 175 Network diagram



As shown in Figure 175, 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 the following elements of Switch A to re-map traffic of different applications to VLANs as per the transmission scheme on the backbone network:
  - GigabitEthernet 1/0/1.
  - GigabitEthernet 1/0/2.
- Configure traffic policing to allocate bandwidth to traffic from different VLANs, as shown in Table 19.

Table 19 Bandwidth allocation

| GE1/0/1 and GE1/0/2 (uplink or downlink) |           |           | GE1/0/3 (uplink or downlink) |          |          | GE1/0/10 (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  |

# 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 the port.
- In a traffic behavior, the traffic policing action cannot be configured together with a priority marking action. Otherwise, a QoS policy that references such a behavior cannot be applied correctly. Priority marking actions include local precedence, drop precedence, 802.1p priority, DSCP, and IP precedence marking.
- Class-behavior associations take effect in the order that they are configured. You must enter traffic mapping class-behavior association before the traffic policing class-behavior association.
- If the VLAN mapping action is referenced first, the device marks the traffic with the new VLAN ID and looks up the QoS policy based on the new VLAN ID. If the policing action is associated with the class for the original VLAN, this renders the policing action useless for the traffic. Likewise, associating the policing action with the class for the original VLAN first renders the VLAN mapping action useless. This is because the device stops searching the QoS policy once a match is found.

## Configuration procedures

### Configuring bandwidth allocation unrelated to VLAN mapping

# Create a class named **vlan201**, and configure SVLAN 201 as the match criterion.

```
<SwitchA> system-view
[SwitchA] traffic classifier vlan201
[SwitchA-classifier-vlan201] if-match service-vlan-id 201
[SwitchA-classifier-vlan201] quit
```

# Create classes named **vlan202** and **vlan203**, and configure SVLAN 202 and SVLAN 203 as their match criteria, respectively.

```
[SwitchA] traffic classifier vlan202
[SwitchA-classifier-vlan202] if-match service-vlan-id 202
[SwitchA-classifier-vlan202] quit
[SwitchA] traffic classifier vlan203
[SwitchA-classifier-vlan203] if-match service-vlan-id 203
[SwitchA-classifier-vlan203] quit
```

# Create a behavior named **car\_vlan201\_downlink** for rate limiting the upstream traffic of VLAN 201 from Branch C. In the behavior, set the CIR to 400000 kbps and CBS to 2500000 bytes (the number of bytes transmitted over 50 ms at the rate of CIR).

```
[SwitchA] traffic behavior car_vlan201_downlink
[SwitchA-behavior-car_vlan201_downlink] car cir 400000 cbs 2500000
[SwitchA-behavior-car_vlan201_downlink] quit
```

# Create behaviors named **car\_vlan202\_downlink** and **car\_vlan203\_downlink**, and configure a traffic policing action in each behavior: set the CIR to 200000 kbps and CBS to 1250000 bytes.

```

[SwitchA] traffic behavior car_vlan202_downlink
[SwitchA-behavior-car_vlan202_downlink] car cir 200000 cbs 1250000
[SwitchA-behavior-car_vlan202_downlink] quit
[SwitchA] traffic behavior car_vlan203_downlink
[SwitchA-behavior-car_vlan203_downlink] car cir 200000 cbs 1250000
[SwitchA-behavior-car_vlan203_downlink] quit

Create a QoS policy named downlink_in_c, and associate the three classes with their specific
behaviors in the QoS policy.
[SwitchA] qos policy downlink_in_c
[SwitchA-qospolicy-downlink_in_c] classifier vlan201 behavior car_vlan201_downlink
[SwitchA-qospolicy-downlink_in_c] classifier vlan202 behavior car_vlan202_downlink
[SwitchA-qospolicy-downlink_in_c] classifier vlan203 behavior car_vlan203_downlink
[SwitchA-qospolicy-downlink_in_c] quit

Apply the QoS policy downlink_in_c to the incoming traffic of GigabitEthernet 1/0/3 to rate limit the
upstream traffic of VLAN 201, VLAN 202, and VLAN 203 from Branch C.
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] qos apply policy downlink_in_c inbound

Apply the QoS policy downlink_in_c to the outgoing traffic of GigabitEthernet 1/0/3 to rate limit the
downstream traffic of VLAN 201, VLAN 202, and VLAN 203 to Branch C.
[SwitchA-GigabitEthernet1/0/3] qos apply policy downlink_in_c outbound

Configure GigabitEthernet 1/0/3 as a trunk port.
[SwitchA-GigabitEthernet1/0/3] port link-type trunk

Assign GigabitEthernet 1/0/3 to VLANs 201 through 203.
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 201 to 203

Remove GigabitEthernet 1/0/3 from VLAN 1.
[SwitchA-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[SwitchA-GigabitEthernet1/0/3] quit

Configure GigabitEthernet 1/0/10 as a trunk port.
[SwitchA] interface GigabitEthernet 1/0/10
[SwitchA-GigabitEthernet1/0/10] port link-type trunk

Assign GigabitEthernet 1/0/10 to VLANs 201 through 203.
[SwitchA-GigabitEthernet1/0/10] port trunk permit vlan 201 to 203

Remove GigabitEthernet 1/0/10 from VLAN 1.
[SwitchA-GigabitEthernet1/0/10] undo port trunk permit vlan 1

```

## Configuring bandwidth allocation related to VLAN mapping

1. Perform the following configurations:

```
Configure GigabitEthernet 1/0/1 as a trunk port.
```

```
[SwitchA] interface GigabitEthernet1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
```

```
Assign GigabitEthernet 1/0/1 to VLANs 1001 through 1003 and VLANs 201 through 203.
```

```
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 1001 to 1003 201 to 203
```

# Remove GigabitEthernet 1/0/1 from VLAN 1.

```
[SwitchA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

# Enable QinQ on GigabitEthernet 1/0/1.

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

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

# Configure GigabitEthernet 1/0/2 as a trunk port.

```
[SwitchA] interface GigabitEthernet1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
```

# Assign GigabitEthernet 1/0/2 to VLANs 1001 through 1003 and VLANs 201 through 203.

```
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 1001 to 1003 201 to 203
```

# Remove GigabitEthernet 1/0/2 from VLAN 1.

```
[SwitchA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
```

# Enable QinQ on GigabitEthernet 1/0/2.

```
[SwitchA-GigabitEthernet1/0/2] qinq enable
```

```
[SwitchA-GigabitEthernet1/0/2] quit
```

## 2. Configure classes and behaviors for performing VLAN mapping for the upstream traffic:

# Create a class named **1001\_to\_201**, and configure CVLAN 1001 as the match criteria. This class is used in the QoS policy that maps VLAN 1001 to VLAN 201.

```
[SwitchA] traffic classifier 1001_to_201
```

```
[SwitchA-classifier-1001_to_201] if-match customer-vlan-id 1001
```

```
[SwitchA-classifier-1001_to_201] quit
```

# Create a behavior named **1001\_to\_201**, and configure the action of marking traffic with SVLAN 201 in the behavior.

```
[SwitchA] traffic behavior 1001_to_201
```

```
[SwitchA-behavior-1001_to_201] remark service-vlan-id 201
```

```
[SwitchA-behavior-1001_to_201] quit
```

# Create classes **1002\_to\_202** and **1003\_to\_203** and behaviors **1002\_to\_202** and **1003\_to\_203**. They are used for mapping VLAN 1002 to VLAN 202 and VLAN 1003 to VLAN 203.

```
[SwitchA] traffic classifier 1002_to_202
```

```
[SwitchA-classifier-1002_to_202] if-match customer-vlan-id 1002
```

```
[SwitchA-classifier-1002_to_202] quit
```

```
[SwitchA] traffic classifier 1003_to_203
```

```
[SwitchA-classifier-1003_to_203] if-match customer-vlan-id 1003
```

```
[SwitchA-classifier-1003_to_203] quit
```

```
[SwitchA] traffic classifier 1003_to_203
```

```
[SwitchA-classifier-1003_to_203] if-match customer-vlan-id 1003
```

```
[SwitchA-classifier-1003_to_203] quit
```

```
[SwitchA] traffic behavior 1003_to_203
```

```
[SwitchA-behavior-1003_to_203] remark service-vlan-id 203
```

```
[SwitchA-behavior-1003_to_203] quit
```

## 3. Configure classes and behaviors for performing VLAN mapping for the downstream traffic:

# Create a class named **201\_to\_1001**, and configure SVLAN 1001 as the match criteria. This class is used in the QoS policy that maps VLAN 201 to VLAN 1001.

```
[SwitchA] traffic classifier 201_to_1001
[SwitchA-classifier-201_to_1001] if-match service-vlan-id 201
[SwitchA-classifier-201_to_1001] quit
```

# Create a behavior named **201\_to\_1001**, and configure the action of marking traffic with CVLAN 1001 in the behavior.

```
[SwitchA] traffic behavior 201_to_1001
[SwitchA-behavior-201_to_1001] remark customer-vlan-id 1001
[SwitchA-behavior-201_to_1001] quit
```

# Create classes **202\_to\_1002** and **203\_to\_1003** and behaviors **202\_to\_1002** and **203\_to\_1003**. They are used for mapping VLAN 202 to VLAN 1002 and VLAN 203 to VLAN 1003.

```
[SwitchA] traffic classifier 202_to_1002
[SwitchA-classifier-202_to_1002] if-match service-vlan-id 202
[SwitchA-classifier-202_to_1002] quit
[SwitchA] traffic behavior 202_to_1002
[SwitchA-behavior-202_to_1002] remark customer-vlan-id 1002
[SwitchA-behavior-202_to_1002] quit
[SwitchA] traffic classifier 203_to_1003
[SwitchA-classifier-203_to_1003] if-match service-vlan-id 203
[SwitchA-classifier-203_to_1003] quit
[SwitchA] traffic behavior 203_to_1003
[SwitchA-behavior-203_to_1003] remark customer-vlan-id 1003
[SwitchA-behavior-203_to_1003] quit
```

#### 4. Configure classes and behaviors to rate limit the upstream traffic from branches:

According to the requirements analysis, the match criteria for rate limiting the upstream traffic from branches are newly marked VLANs. Therefore, you can use the traffic classes for VLAN 201, VLAN 202, and VLAN 203, which are **201\_to\_1001**, **202\_to\_1002**, and **203\_to\_1003** in this example. The behaviors for policing the traffic can be **car\_vlan201\_downlink**, **car\_vlan202\_downlink**, and **car\_vlan203\_downlink**, which are configured in "[Configuring bandwidth allocation unrelated to VLAN mapping](#)."

#### 5. Configure classes and behaviors for rate limiting the downstream traffic sent to branches:

# Create a class named **vlan201\_downlink**, and configure SVLAN 1001 as the match criteria.

```
[SwitchA] traffic classifier vlan201_downlink
[SwitchA-classifier-vlan201_downlink] if-match service-vlan-id 1001
[SwitchA-classifier-vlan201_downlink] quit
```

---

#### NOTE:

When you configure a class for rate limiting the downstream traffic, you must use the **service-vlan-id** criterion. The VLAN specified for the criterion, however, should be the marked customer-side VLAN ID, for example, VLAN 1001.

---

# Create classes **vlan202\_downlink** and **vlan203\_downlink** in the same way.

```
[SwitchA] traffic classifier vlan202_downlink
[SwitchA-classifier-vlan202_downlink] if-match service-vlan-id 1002
[SwitchA-classifier-vlan202_downlink] quit
[SwitchA] traffic classifier vlan203_downlink
```

```
[SwitchA-classifier-vlan203_downlink] if-match service-vlan-id 1003
[SwitchA-classifier-vlan203_downlink] quit
```

Because the rate limit requirements for the downstream traffic are the same as those for the upstream traffic, you can use the behaviors **car\_vlan201\_downlink**, **car\_vlan202\_downlink**, and **car\_vlan203\_downlink**.

6. Configure classes and behaviors for rate-limiting the upstream traffic to the backbone network:

The match criteria for rate-limiting the upstream traffic are newly marked VLANs (VLAN 201, VLAN 202, and VLAN 203). Therefore, you can use classes **201\_to\_1001**, **202\_to\_1002**, and **203\_to\_1003**.

# Create a behavior named **car\_vlan201\_uplink** for rate limiting the upstream traffic of VLAN 201 on Switch A. In the behavior, set the CIR to 100000 kbps and CBS to 625000 bytes (the number of bytes transmitted over 50 ms at the rate of CIR).

```
[SwitchA] traffic behavior car_vlan201_uplink
[SwitchA-behavior-car_vlan201_uplink] car cir 100000 cbs 625000
[SwitchA-behavior-car_vlan201_uplink] quit
```

# Create behaviors named **car\_vlan202\_uplink** and **car\_vlan203\_uplink** for rate limiting upstream traffic of VLAN 202 and VLAN 203. In the behavior **car\_vlan202\_uplink**, set the CIR to 60000 kbps and CBS to 375000 bytes. In the behavior **car\_vlan203\_uplink**, set the CIR to 40000 kbps and CBS to 250000 bytes.

```
[SwitchA] traffic behavior car_vlan202_uplink
[SwitchA-behavior-car_vlan202_uplink] car cir 60000 cbs 375000
[SwitchA-behavior-car_vlan202_uplink] quit
[SwitchA] traffic behavior car_vlan203_uplink
[SwitchA-behavior-car_vlan203_uplink] car cir 40000 cbs 250000
[SwitchA-behavior-car_vlan203_uplink] quit
```

7. Configure classes and behaviors to rate limit the downstream traffic from the backbone network:

The match criteria for rate limiting the downstream traffic from the backbone network are newly marked VLANs (VLAN 201, VLAN 202, and VLAN 203). Therefore, you can use classes **201\_to\_1001**, **202\_to\_1002**, and **203\_to\_1003**.

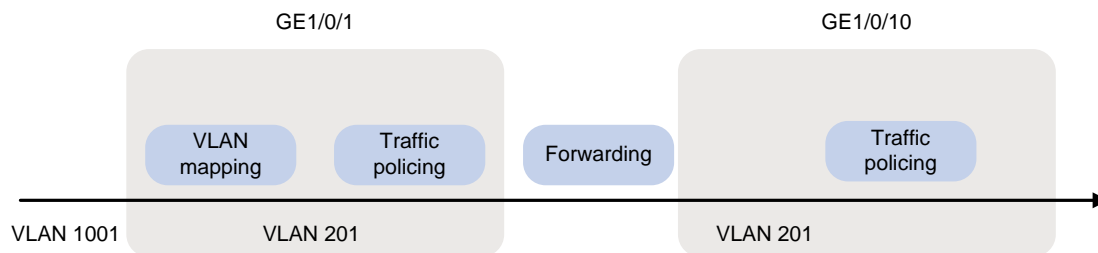
Because the rate limit requirements for the downstream traffic are the same as those for the upstream traffic, you can use the behaviors **car\_vlan201\_uplink**, **car\_vlan202\_uplink**, and **car\_vlan203\_uplink**.

8. Configure and apply the QoS policies for upstream traffic.

[Figure 176](#) shows how the switches process the upstream traffic from a branch to the backbone network. The figure uses VLAN 1001 as an example.



Figure 176 Upstream traffic processing



# Create a QoS policy named **downlink\_in**, and configure the following class-behavior associations in this order:

- The VLAN mapping class-behavior associations.
- The traffic policing class-behavior associations that use the newly marked VLANs as the match criteria.

```
[SwitchA] qos policy downlink_in
[SwitchA-qospolicy-downlink_in] classifier 1001_to_201 behavior 1001_to_201
[SwitchA-qospolicy-downlink_in] classifier 1002_to_202 behavior 1002_to_202
[SwitchA-qospolicy-downlink_in] classifier 1003_to_203 behavior 1003_to_203
[SwitchA-qospolicy-downlink_in] classifier 201_to_1001 behavior
car_vlan201_downlink
[SwitchA-qospolicy-downlink_in] classifier 202_to_1002 behavior
car_vlan202_downlink
[SwitchA-qospolicy-downlink_in] classifier 203_to_1003 behavior
car_vlan203_downlink
[SwitchA-qospolicy-downlink_in] quit
```

# Apply the QoS policy **downlink\_in** to the incoming traffic of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[SwitchA] interface GigabitEthernet1/0/1
[SwitchA-GigabitEthernet1/0/1] qos apply policy downlink_in inbound
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet1/0/2
[SwitchA-GigabitEthernet1/0/2] qos apply policy downlink_in inbound
[SwitchA-GigabitEthernet1/0/2] quit
```

# Create a QoS policy named **uplink\_out**, and associate the classes and behaviors configured to rate-limit the upstream traffic to the backbone network.

```
[SwitchA] qos policy uplink_out
[SwitchA-qospolicy-uplink_out] classifier 201_to_1001 behavior car_vlan201_uplink
[SwitchA-qospolicy-uplink_out] classifier 202_to_1002 behavior car_vlan202_uplink
[SwitchA-qospolicy-uplink_out] classifier 203_to_1003 behavior car_vlan203_uplink
[SwitchA-qospolicy-downlink_in] quit
```

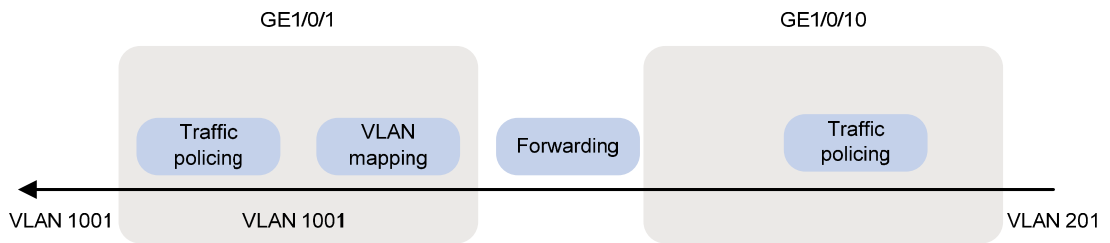
# Apply QoS policy **uplink\_out** to the outgoing traffic of GigabitEthernet 1/0/10.

```
[SwitchA] interface GigabitEthernet1/0/10
[SwitchA-GigabitEthernet1/0/10] qos apply policy uplink_out outbound
```

9. Configure and apply the QoS policies for downstream traffic:

Figure 177 shows how the switches process the downstream traffic from a branch to the backbone network. The figure uses VLAN 1001 as an example.

**Figure 177 Downstream traffic processing**



# Create a QoS policy named **uplink\_in**, and associate the classes and behaviors configured to rate limit the downstream traffic from the backbone network.

```
[SwitchA] qos policy uplink_in
[SwitchA-qospolicy-uplink_in] classifier 201_to_1001 behavior car_vlan201_uplink
[SwitchA-qospolicy-uplink_in] classifier 202_to_1002 behavior car_vlan202_uplink
[SwitchA-qospolicy-uplink_in] classifier 203_to_1003 behavior car_vlan203_uplink
[SwitchA-qospolicy-uplink_in] quit
```

# Apply the QoS policy **uplink\_in** to the incoming traffic of GigabitEthernet 1/0/10.

```
[SwitchA] interface GigabitEthernet1/0/10
[SwitchA-GigabitEthernet1/0/10] qos apply policy uplink_in inbound
```

# Create a QoS policy named **downlink\_out**, and configure the following class-behavior associations in this order:

- o The VLAN mapping class-behavior associations.
- o The traffic policing class-behavior associations that rate limit the downstream traffic to branches.

```
[SwitchA] qos policy downlink_out
[SwitchA-qospolicy-downlink_out] classifier 201_to_1001 behavior 201_to_1001
[SwitchA-qospolicy-downlink_out] classifier 202_to_1002 behavior 202_to_1002
[SwitchA-qospolicy-downlink_out] classifier 203_to_1003 behavior 203_to_1003
[SwitchA-qospolicy-downlink_out] classifier vlan201_downlink behavior
car_vlan201_downlink
[SwitchA-qospolicy-downlink_out] classifier vlan202_downlink behavior
car_vlan202_downlink
[SwitchA-qospolicy-downlink_out] classifier vlan203_downlink behavior
car_vlan203_downlink
[SwitchA-qospolicy-downlink_in] quit
```

# Apply the QoS policy **downlink\_out** to the outgoing traffic of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[SwitchA] interface GigabitEthernet1/0/1
[SwitchA-GigabitEthernet1/0/1] qos apply policy downlink_out outbound
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet1/0/2
[SwitchA-GigabitEthernet1/0/2] qos apply policy downlink_out outbound
[SwitchA-GigabitEthernet1/0/2] quit
```

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
traffic classifier vlan203_downlink operator and
 if-match service-vlan-id 1003
traffic classifier 1002_to_202 operator and
 if-match customer-vlan-id 1002
traffic classifier 201_to_1001 operator and
 if-match service-vlan-id 201
traffic classifier 1003_to_203 operator and
 if-match customer-vlan-id 1003
traffic classifier 203_to_1003 operator and
 if-match service-vlan-id 203
traffic classifier vlan201 operator and
 if-match service-vlan-id 201
traffic classifier vlan201_downlink operator and
 if-match service-vlan-id 1001
traffic classifier vlan202 operator and
 if-match service-vlan-id 202
traffic classifier vlan202_downlink operator and
 if-match service-vlan-id 1002
traffic classifier 202_to_1002 operator and
 if-match service-vlan-id 202
traffic classifier 1001_to_201 operator and
 if-match customer-vlan-id 1001
traffic classifier vlan203 operator and
 if-match service-vlan-id 203
#
traffic behavior car_vlan201_downlink
 car cir 400000 cbs 2500000 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan202_downlink
 car cir 200000 cbs 1250000 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan203_downlink
 car cir 200000 cbs 1250000 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan201_uplink
 car cir 100000 cbs 625000 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan202_uplink
 car cir 60000 cbs 375000 ebs 512 green pass red discard yellow pass
traffic behavior car_vlan203_uplink
 car cir 40000 cbs 250000 ebs 512 green pass red discard yellow pass
traffic behavior 1002_to_202
 remark service-vlan-id 202
traffic behavior 201_to_1001
 remark customer-vlan-id 1001
traffic behavior 1003_to_203
 remark service-vlan-id 203
```

```

traffic behavior 203_to_1003
 remark customer-vlan-id 1003
traffic behavior 202_to_1002
 remark customer-vlan-id 1002
traffic behavior 1001_to_201
 remark service-vlan-id 201
#
qos policy uplink_in
 classifier 201_to_1001 behavior car_vlan201_uplink
 classifier 202_to_1002 behavior car_vlan202_uplink
 classifier 203_to_1003 behavior car_vlan203_uplink
qos policy uplink_out
 classifier 201_to_1001 behavior car_vlan201_uplink
 classifier 202_to_1002 behavior car_vlan202_uplink
 classifier 203_to_1003 behavior car_vlan203_uplink
qos policy downlink_in
 classifier 1001_to_201 behavior 1001_to_201
 classifier 1002_to_202 behavior 1002_to_202
 classifier 1003_to_203 behavior 1003_to_203
 classifier 201_to_1001 behavior car_vlan201_downlink
 classifier 202_to_1002 behavior car_vlan202_downlink
 classifier 203_to_1003 behavior car_vlan203_downlink
qos policy downlink_in_c
 classifier vlan201 behavior car_vlan201_downlink
 classifier vlan202 behavior car_vlan202_downlink
 classifier vlan203 behavior car_vlan203_downlink
qos policy downlink_out
 classifier 201_to_1001 behavior 201_to_1001
 classifier 202_to_1002 behavior 202_to_1002
 classifier 203_to_1003 behavior 203_to_1003
 classifier vlan201_downlink behavior car_vlan201_downlink
 classifier vlan202_downlink behavior car_vlan202_downlink
 classifier vlan203_downlink behavior car_vlan203_downlink
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 201 to 203 1001 to 1003
 qinq enable
 qos apply policy downlink_in inbound
 qos apply policy downlink_out outbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 201 to 203 1001 to 1003

```

```

qinq enable
qos apply policy downlink_in inbound
qos apply policy downlink_out outbound
#
interface GigabitEthernet1/0/10
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 201 to 203
qos apply policy uplink_in inbound
qos apply policy uplink_out outbound

```

## Example: Configuring aggregate CAR

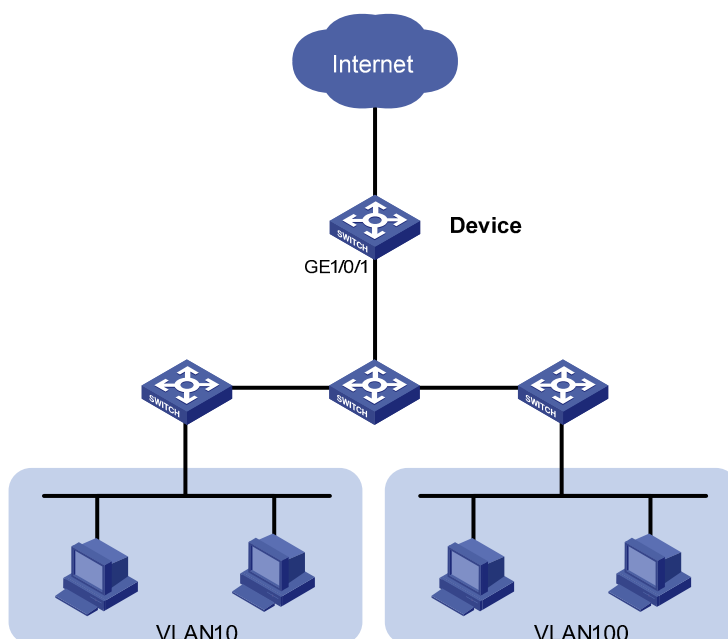
### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

### Network requirements

As shown in [Figure 178](#), configure aggregate CAR on 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 178 Network diagram**



## Configuration restrictions and guidelines

In a traffic behavior, the traffic policing action cannot be configured together with a priority marking action. Otherwise, a QoS policy that references such a behavior cannot be applied correctly. Priority marking actions include local precedence, drop precedence, 802.1p priority, DSCP, and IP precedence marking

## 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 the device.

# Configure GigabitEthernet 1/0/1 as a trunk port.

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-type trunk
```

# Assign it to VLANs 10 through 100.

```
[Device-GigabitEthernet1/0/1] port trunk permit vlan 10 100
```

# Remove it from VLAN 1.

```
[Device-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Device-GigabitEthernet1/0/1] quit
```

# Create an aggregate CAR action.

```
[Device] qos car aggcarr-1 aggregative cir 200000 red discard
```

# Configure class 1 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 behavior 1 with the aggregate CAR action.

```
[Device] traffic behavior 1
[Device-behavior-1] car name aggcarr-1
[Device-behavior-1] quit
```

# Configure class 2 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 aggcarr-1
[Device-behavior-2] quit
```

# Create a QoS policy named **car**, and associate the classes with the behaviors in the QoS policy.

```
[Device] qos policy car
[Device-qospolicy-car] classifier 1 behavior 1
```

```
[Device-qospolicy-car] classifier 2 behavior 2
[Device-qospolicy-car] quit

Apply the QoS policy car to the incoming traffic of GigabitEthernet 1/0/1.
[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy car inbound
```

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
qos car aggcar-1 aggregative cir 20000 cbs 1250000 ebs 512 green pass yellow pa
ss red discard
#
traffic classifier 1 operator and
if-match service-vlan-id 10
traffic classifier 2 operator and
if-match service-vlan-id 100
#
traffic behavior 1
car name aggcar-1
traffic behavior 2
car name aggcar-1
#
qos policy car
classifier 1 behavior 1
classifier 2 behavior 2
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 100
qos apply policy car inbound
```

# GTS and rate limiting configuration examples

This chapter provides GTS and rate limiting configuration examples.

## Example: Configuring GTS and rate limiting

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

### Network requirements

As shown in [Figure 179](#), a company connects its branch and its headquarters through a dedicated line. The dedicated line mainly transmits the FTP traffic, service application traffic, and IP voice traffic.

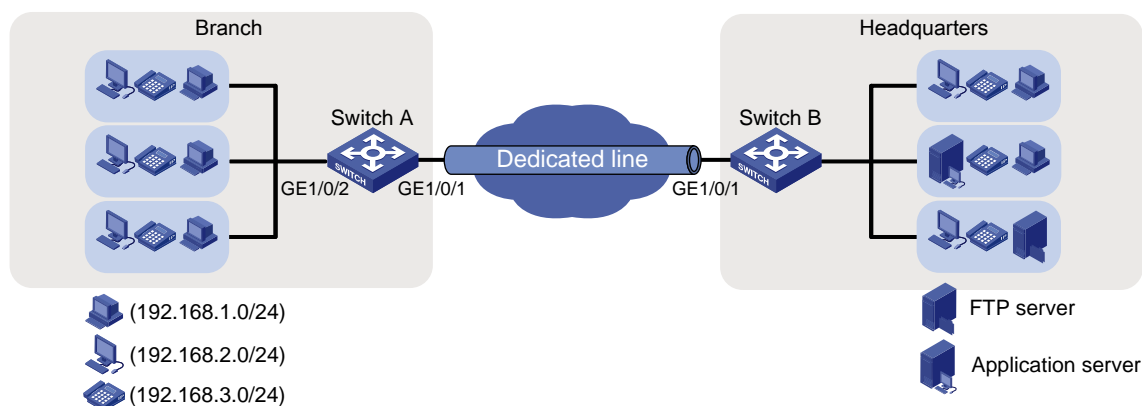
Due to limited dedicated line bandwidth, configure traffic policing on the edge device Switch B of the headquarters, as follows:

- Set the CIR to 10 Mbps for IP voice traffic.
- Set the CIR to 3 Mbps for service application traffic.
- Set the CIR to 7 Mbps for FTP traffic.

To cooperate with the traffic policing configured at the headquarters, configure traffic shaping on edge device Switch A of the branch to buffer the excess bursty traffic and to 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 179 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 not provided. You must use priority marking to manually assign packets to different queues.
- To manually assign packets to queues and keep the packets unchanged, you must mark local precedence values for packets.

## Configuration procedures

---

### ! IMPORTANT:

Before you configure GTS and rate limiting, make sure the network in [Figure 179](#) is reachable. Information about implementing connectivity on Switch A and Switch B is not shown.

---

### Configuring priority marking

1. Create three classes on Switch A to match the three types of traffic by source IP address:

# Configure IPv4 basic ACL 2000 to match the voice 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 service application 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 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.
```

```
[SwitchA] qos policy shaping
```

```
Associate class voice with traffic behavior voice in the QoS policy to assign the voice traffic to queue 6.
```

```
[SwitchA-qospolicy-shaping] classifier voice behavior voice
```

```
Associate class service with traffic behavior service in the QoS policy to assign the service application traffic to queue 4.
```

```
[SwitchA-qospolicy-shaping] classifier service behavior service
```

```
Associate class ftp with traffic behavior ftp in the QoS policy to assign the FTP traffic to queue 2.
```

```
[SwitchA-qospolicy-shaping] classifier ftp behavior ftp
```

```
[SwitchA-qospolicy-shaping] quit
```

```
Apply the QoS policy to the incoming traffic of GigabitEthernet 1/0/2.
```

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] qos apply policy shaping inbound
[SwitchA-GigabitEthernet1/0/2] quit
```

## Configuring GTS

```
Configure traffic shaping on port GigabitEthernet 1/0/1, and set the CIR to 10000 kbps for queue 6.
```

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos gts queue 6 cir 10000
```

```
Configure traffic shaping on port GigabitEthernet 1/0/1, and set the CIR to 3000 kbps for queue 4.
```

```
[SwitchA-GigabitEthernet1/0/1] qos gts queue 4 cir 3000
```

```
Configure traffic shaping on port GigabitEthernet 1/0/1, and set the CIR to 7000 kbps for queue 2.
```

```
[SwitchA-GigabitEthernet1/0/1] qos gts queue 2 cir 7000
```

## Configuring rate limiting

```
Configure rate limiting in the outbound direction of GigabitEthernet 1/0/1 (20000 kbps CIR).
```

```
[SwitchA-GigabitEthernet1/0/1] qos lr outbound cir 20000
```

## Verifying the configuration

# Use the **display qos gts interface** command to display traffic shaping configuration.

```
<Sysname> display qos gts interface
Interface: GigabitEthernet1/0/1
Rule(s): If-match queue 6
CIR 10000 (kbps), CBS 625152 (byte)
Rule(s): If-match queue 4
CIR 7000 (kbps), CBS 437760 (byte)
Rule(s): If-match queue 2
CIR 3000 (kbps), CBS 187904 (byte)
```

# Use the **display qos lr interface** command to display the rate limiting configuration of a port.

```
<Sysname> display qos lr interface
Interface: GigabitEthernet1/0/1
Direction: Outbound
CIR 20000 (kbps), CBS 1250304 (byte)
```

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

```
#
acl number 2000
 rule 0 permit source 192.168.3.0 0.0.0.255
acl number 2001
 rule 0 permit source 192.168.2.0 0.0.0.255
#
acl number 3000
 rule 0 permit tcp source 192.168.1.0 0.0.0.255 destination-port eq ftp-data
#
traffic classifier service operator and
 if-match acl 2001
traffic classifier ftp operator and
 if-match acl 3000
traffic classifier voice operator and
 if-match acl 2000
#
traffic behavior service
 remark local-precedence 4
traffic behavior ftp
 remark local-precedence 2
traffic behavior voice
 remark local-precedence 6
#
qos policy shaping
 classifier voice behavior voice
```

```
classifier service behavior service
classifier ftp behavior ftp
#
interface GigabitEthernet1/0/1
port link-mode bridge
qos lr outbound cir 20000 cbs 1250304
qos gts queue 6 cir 10000 cbs 625152
qos gts queue 4 cir 7000 cbs 437760
qos gts queue 2 cir 3000 cbs 187904
#
interface GigabitEthernet1/2/0/2
port link-mode bridge
qos apply policy shaping inbound
```

# Priority and queue scheduling configuration examples

This chapter provides priority mapping, priority marking, and queue scheduling configuration examples.

## Example: Configuring priority mapping and queue scheduling

### Applicable product matrix

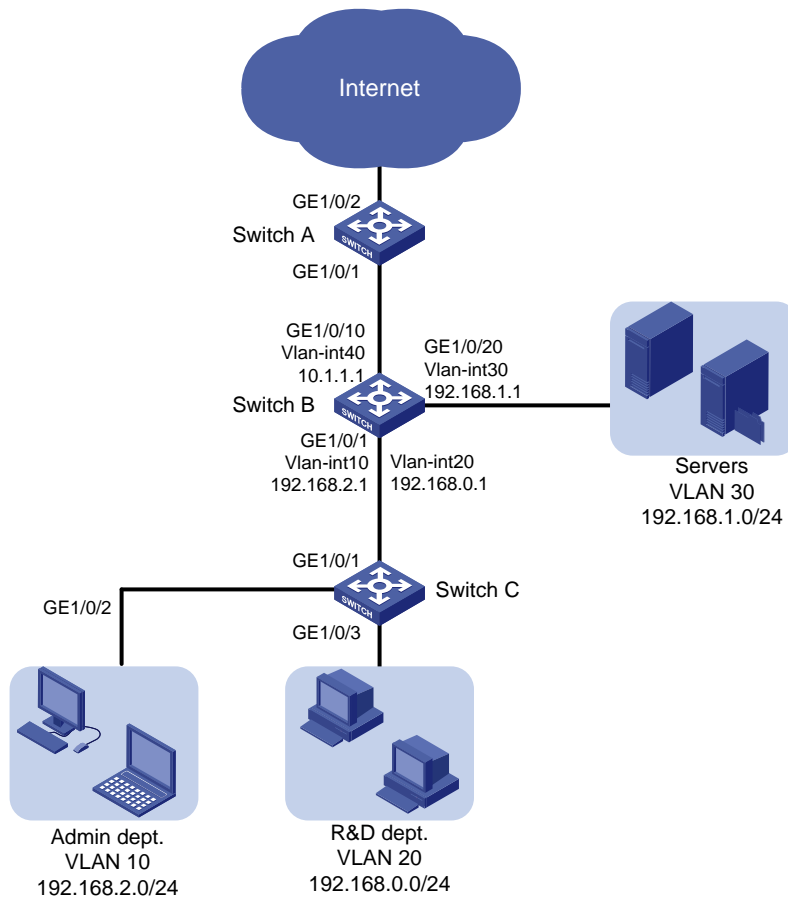
| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

### Network requirements

The network diagram of a company is as shown in [Figure 180](#). 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, and the traffic from the R&D department is scheduled when no traffic from the Administration department exists.
- The Internet-accessing traffic includes the following types: HTTP, FTP, and Email, with the DSCP values 33, 35, and 27, respectively. Transmit the three types of traffic in the following priority order: HTTP > FTP > Email. When congestion occurs, the three types of traffic are transmitted in the ratio of 2:1:1.

Figure 180 Network diagram



## Requirements analysis

### Priority configuration for the internal network traffic

To prioritize packets by department, configure different port priorities for the ports connected to the two departments.

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.

To meet the packet scheduling ratio when congestion occurs, configure WRR on port GigabitEthernet 1/0/20 of Switch B and configure different weights for queues.

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 completely 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 meet requirements of determining 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 GigabitEthernet 1/0/2 to VLAN 10. Set the port priority to 6 for the port, so that the traffic from the Administration department is marked with 802.1p priority value 6.

```
[SwitchC] interface GigabitEthernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port access vlan 10
[SwitchC-GigabitEthernet1/0/2] qos priority 6
[SwitchC-GigabitEthernet1/0/2] quit
```

# Assign port GigabitEthernet 1/0/3 to VLAN 20. Set the port priority to 4 for the port, so that the traffic from the R&D department is marked with 802.1p priority value 4.

```
[SwitchC] interface GigabitEthernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] port access vlan 20
[SwitchC-GigabitEthernet1/0/3] qos priority 4
[SwitchC-GigabitEthernet1/0/3] quit
```

# 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 GigabitEthernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[SwitchC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchC-GigabitEthernet1/0/1] quit
```

#### 2. Configure Switch B:

# Create VLANs 10, 20, 30, and 40.

```
<SwitchB> system-view
[SwitchB] vlan 10
[SwitchB-vlan10] quit
[SwitchB] vlan 20
```

```

[SwitchB-vlan20] quit
[SwitchB] vlan 30
[SwitchB-vlan30] quit
[SwitchB] vlan 40
[SwitchB-vlan40] quit
Configure GigabitEthernet 1/0/1 as a trunk port.
<SwitchB> system-view
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
Assign the port to VLANs 10 and 20.
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 10 20
Remove the port from VLAN 1.
[SwitchB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
Configure port GigabitEthernet 1/0/1 to trust the 802.1p priorities of received packets. 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-GigabitEthernet1/0/1] qos trust dot1p
[SwitchB-GigabitEthernet1/0/1] quit
Assign port GigabitEthernet 1/0/10 to VLAN 40.
[SwitchB] interface GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] port access vlan 40
Assign port GigabitEthernet 1/0/20 to VLAN 30.
[SwitchB] interface GigabitEthernet 1/0/20
[SwitchB-GigabitEthernet1/0/20] port access vlan 30
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 GigabitEthernet 1/0/20.
[SwitchB] interface GigabitEthernet 1/0/20
[SwitchB-GigabitEthernet1/0/20] qos wrr byte-count
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-GigabitEthernet1/0/20] qos wrr 4 group 1 byte-count 2
[SwitchB-GigabitEthernet1/0/20] qos wrr 6 group 1 byte-count 4
[SwitchB-GigabitEthernet1/0/20] quit

```

---

#### NOTE:

The S5500-SI switches do not support the keyword. Use the **qos wrr** command to enable packet-based WRR and the **qos wrr weight** command to set weights for queues.

---

## Configuring transmission priorities for the traffic to the Internet

1. Configure Switch B:  

```

Enable SP queuing on port GigabitEthernet 1/0/10.
[SwitchB] interface GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] qos sp

```
2. Configure Switch A:



# Configure port GigabitEthernet 1/0/1 to trust the DSCP values of received packets.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos trust dscp
```

# 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 to queues 5, 4, and 3, respectively.

# Enable byte-count WRR on GigabitEthernet 1/0/2, and set the weights of the three queues in the ratio of 2:1:1 (for example, 6, 3, and 3).

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] qos wrr byte-count
[SwitchA-GigabitEthernet1/0/2] qos wrr 5 group 1 byte-count 6
[SwitchA-GigabitEthernet1/0/2] qos wrr 4 group 1 byte-count 3
[SwitchA-GigabitEthernet1/0/2] qos wrr 3 group 1 byte-count 3
```

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```
#
qos map-table dscp-dot1p
 import 33 export 5
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 qos trust dscp
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 qos wrr byte-count
 qos wrr 5 group 1 byte-count 6
 qos wrr 4 group 1 byte-count 3
 qos wrr 3 group 1 byte-count 3
```

- Switch B:

```
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
interface GigabitEthernet1/0/1
 port link-mode bridge
```

```

port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20
qos trust dot1p
#
interface GigabitEthernet1/0/10
port link-mode bridge
port access vlan 40
#
interface GigabitEthernet1/0/20
port link-mode bridge
port access vlan 30
qos wrr byte-count
qos wrr 6 group 1 byte-count 4
qos wrr 4 group 1 byte-count 2

```

- Switch C:

```

#
vlan 10
#
vlan 20
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 10
qos priority 6
#
interface GigabitEthernet1/0/3
port link-mode bridge
port access vlan 20
qos priority 4

```

## Example: Configuring priority marking and queue scheduling

### Applicable product matrix

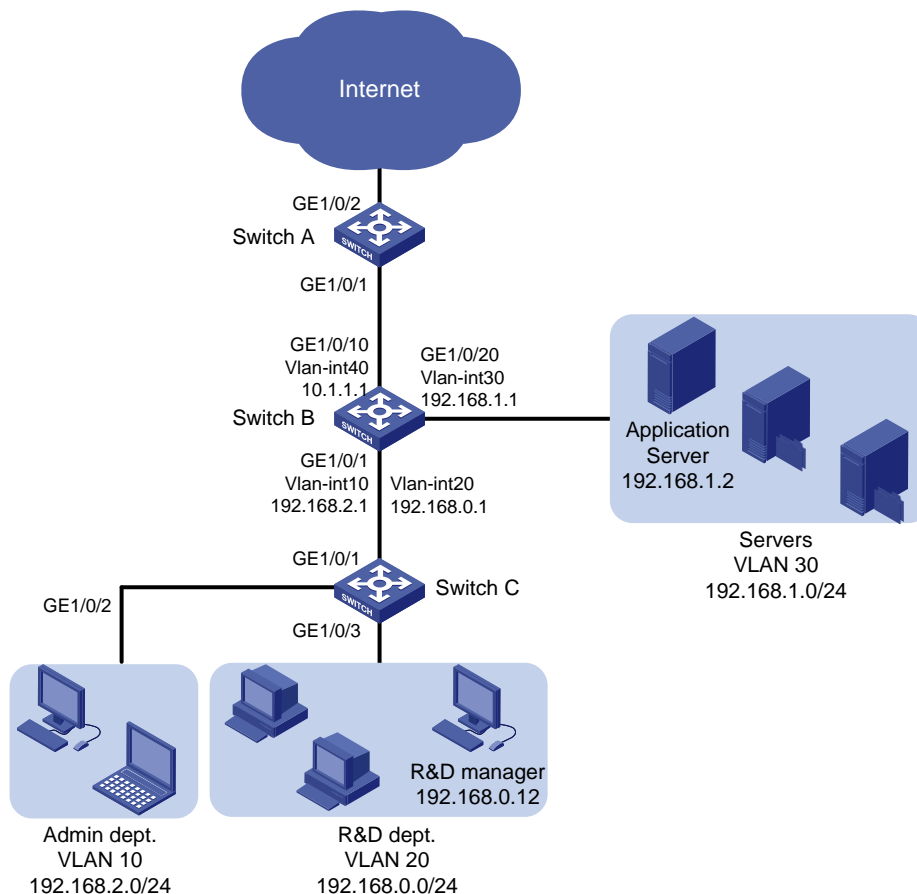
| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

The network diagram of a company is as shown in [Figure 181](#). Tune the internal network traffic and Internet-accessing traffic of the company on each device 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. Transmit the three types of traffic in the following priority order: HTTP>FTP>Email. When congestion occurs, the three types of traffic are transmitted in the ratio of 2:1:1. The email traffic of the Administration department is assigned the same priority as the HTTP traffic.

**Figure 181 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, configure priority marking.
  - Configure priority marking in a QoS policy:
    - Configure a class to match the traffic destined to the application server IP address.
    - Configure a traffic behavior to mark local precedence for the class of traffic, so that all traffic that accesses the application server can be assigned to an individual queue.
  - Configure SP + WRR queuing on port GigabitEthernet 1/0/20 to assign the queue to the SP group.
- 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 on Switch C.As a result, when the traffic from the R&D department manager reaches Switch B, the traffic can be assigned the same local precedence value as the traffic from the Administration department.
- For the email traffic from the Administration department, you can perform the following configurations:
  - Configure a class to match the traffic with DSCP value 27.
  - Configure a priority marking behavior to mark the class of traffic with the same local precedence value as the HTTP traffic.
- 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 GigabitEthernet 1/0/2 to VLAN 10. Set the port priority to 6 for the port, so that the
traffic from the Administration department is marked with 802.1p priority value 6.
[SwitchC] interface GigabitEthernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port access vlan 10
[SwitchC-GigabitEthernet1/0/2] qos priority 6
[SwitchC-GigabitEthernet1/0/2] quit

Assign port GigabitEthernet 1/0/3 to VLAN 20. Set the port priority to 4 for the port, so that the
traffic from the R&D department is marked with 802.1p priority value 4.
[SwitchC] interface GigabitEthernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] port access vlan 20
[SwitchC-GigabitEthernet1/0/3] qos priority 4
[SwitchC-GigabitEthernet1/0/3] quit

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 GigabitEthernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[SwitchC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchC-GigabitEthernet1/0/1] quit

```

## 2. Configure Switch B:

# Create VLANs 10, 20, 30, and 40.

```

<SwitchB> system-view
[SwitchB] vlan 10
[SwitchB-vlan10] quit
[SwitchB] vlan 20
[SwitchB-vlan20] quit
[SwitchB] vlan 30
[SwitchB-vlan30] quit
[SwitchB] vlan 40
[SwitchB-vlan40] quit

```

# Configure GigabitEthernet 1/0/1 as a trunk port.

```

<SwitchB> system-view
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk

```

# Assign the port to VLANs 10 and 20.

```

[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 10 20

```

# Remove the port from VLAN 1.

```

[SwitchB-GigabitEthernet1/0/1] undo port trunk permit vlan 1

```

# Configure port GigabitEthernet 1/0/1 to trust the 802.1p priorities of received packets. 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-GigabitEthernet1/0/1] qos trust dot1p
[SwitchB-GigabitEthernet1/0/1] quit

```

```

Assign port GigabitEthernet 1/0/10 to VLAN 40.
[SwitchB] interface GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] port access vlan 40
Assign port GigabitEthernet 1/0/20 to VLAN 30.
[SwitchB] interface GigabitEthernet 1/0/20
[SwitchB-GigabitEthernet1/0/20] port access vlan 30
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 GigabitEthernet 1/0/1.
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] qos apply policy app_server inbound
[SwitchB-GigabitEthernet1/0/1] quit
Enable byte-count SP + WRR queuing on egress port GigabitEthernet 1/0/20.
[SwitchB] interface GigabitEthernet 1/0/20
[SwitchB-GigabitEthernet1/0/20] qos wrr byte-count
Configure queue 7 as an SP queue.
[SwitchB-GigabitEthernet1/0/20] qos wrr 7 group sp
Configure queues 4 and 6 as WRR queues. Configure the weight of queue 6 as two times that
of queue 4. In this example, set the weight value to 4 for queue 6 and 2 for queue 4.
[SwitchB-GigabitEthernet1/0/20] qos wrr 6 group 1 byte-count 4
[SwitchB-GigabitEthernet1/0/20] qos wrr 4 group 1 byte-count 2

```

---

**NOTE:**

The S5500-SI switches do not support the keyword. Use the **qos wrr** command to enable packet-based WRR and the **qos wrr weight** command to set weights for queues.

---

## Configuring transmission priorities for the traffic to the Internet

### 1. Configure Switch C:

```
Configure IPv4 basic ACL 2000 to match the traffic with source IP address 192.168.0.12.
[SwitchC] acl number 2000
[SwitchC-acl-basic-2000] rule permit source 192.168.0.12 0
[SwitchC-acl-basic-2000] quit

Create a class named rd_manager, and use IPv4 ACL 2000 as the match criterion in the class.
[SwitchC] traffic classifier rd_manager
[SwitchC-classifier-rd_manager] if-match acl 2000
[SwitchC-classifier-rd_manager] quit

Create a behavior named rd_manager, and configure the action of setting the 802.1p priority
value to 6 for the behavior.
[SwitchC] traffic behavior rd_manager
[SwitchC-behavior-rd_manager] remark dot1p 6
[SwitchC-behavior-rd_manager] quit

Create a QoS policy named rd_manager, and associate class rd_manager with traffic behavior
rd_manager in the QoS policy.
[SwitchC] qos policy rd_manager
[SwitchC-qospolicy-rd_manager] classifier rd_manager behavior rd_manager
[SwitchC-qospolicy-rd_manager] quit

Apply QoS policy rd_manager to the incoming traffic of GigabitEthernet 1/0/3.
[SwitchC] interface GigabitEthernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] qos apply policy rd_manager inbound
[SwitchC-GigabitEthernet1/0/3] quit
```

### 2. Configure Switch B:

```
Enable SP queuing on port GigabitEthernet 1/0/10.
[SwitchB] interface GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] qos sp
```

### 3. Configure Switch A:

```
Configure port GigabitEthernet 1/0/1 to trust the DSCP values of received packets.
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos trust dscp

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 above assigns the three types of packets to queues 5, 4, and 3.

# Enable byte-count WRR on GigabitEthernet 1/0/2, and set the weights for the three queues in the ratio of 2:1:1 (for example, 6, 3, and 3).

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] qos wrr byte-count
[SwitchA-GigabitEthernet1/0/2] qos wrr 5 group 1 byte-count 6
[SwitchA-GigabitEthernet1/0/2] qos wrr 4 group 1 byte-count 3
[SwitchA-GigabitEthernet1/0/2] qos wrr 3 group 1 byte-count 3
```

```

[SwitchA-GigabitEthernet1/0/2] quit
Configure IPv4 advanced ACL 3000 to match the traffic that is sourced from network segment
192.168.2.0/24 that carries DSCP value 27.
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule permit ip dscp 27 source 192.168.2.0 0.0.0.255
[SwitchA-acl-adv-3000] quit
Create a class named admin_email, and use IPv4 ACL 3000 as the match criterion in the class.
[SwitchA] traffic classifier admin_email
[SwitchA-classifier-admin_email] if-match acl 3000
[SwitchA-classifier-admin_email] quit
Create a behavior named admin_email, and configure the action of setting the local precedence
value to 5 for the behavior.
[SwitchA] traffic behavior admin_email
[SwitchA-behavior-admin_email] remark local-precedence 5
[SwitchA-behavior-admin_email] quit
Create a QoS policy named admin_email, and associate class admin_email with traffic
behavior admin_email in the QoS policy.
[SwitchA] qos policy admin_email
[SwitchA-qospolicy-admin_email] classifier admin_email behavior admin_email
[SwitchA-qospolicy-admin_email] quit
Apply QoS policy admin_email to the incoming traffic of GigabitEthernet 1/0/1.
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos apply policy admin_email inbound
[SwitchA-GigabitEthernet1/0/1] quit

```

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```

#
acl number 3000
 rule 0 permit ip source 192.168.2.0 0.0.0.255 dscp 27
#
traffic classifier admin_email operator and
 if-match acl 3000
#
traffic behavior admin_email
 remark local-precedence 5
#
qos policy admin_email
 classifier admin_email behavior admin_email
#
qos map-table dscp-dot1p
 import 33 export 5
#
interface GigabitEthernet1/0/1
 port link-mode bridge

```



```

qos apply policy admin_email inbound
qos trust dscp
#
interface GigabitEthernet1/0/2
port link-mode bridge
qos wrr byte-count
qos wrr 5 group 1 byte-count 6
qos wrr 4 group 1 byte-count 3
qos wrr 3 group 1 byte-count 3

```

- Switch B:

```

#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
acl number 3000
rule 0 permit ip destination 192.168.1.2 0
#
traffic classifier app_server operator and
if-match acl 3000
#
traffic behavior app_server
remark local-precedence 7
#
qos policy app_server
classifier app_server behavior app_server
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20
qos apply policy app_server inbound
qos trust dot1p
#
interface GigabitEthernet1/0/10
port link-mode bridge
port access vlan 40
#
interface GigabitEthernet1/0/20
port link-mode bridge
port access vlan 30
qos wrr byte-count
qos wrr 7 group sp

```

```
qos wrr 6 group 1 byte-count 4
qos wrr 4 group 1 byte-count 2
```

- Switch C:

```
#
vlan 10
#
vlan 20
#
acl number 2000
 rule 0 permit source 192.168.0.12 0
#
traffic classifier rd_manager operator and
 if-match acl 2000
#
traffic behavior rd_manager
 remark dot1p 6
#
qos policy rd_manager
 classifier rd_manager behavior rd_manager
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
 qos priority 6
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 20
 qos apply policy rd_manager inbound
 qos priority 4
```

# User profile configuration examples

This chapter provides configuration examples for applying QoS policies to authenticated users through user profiles.

## Example: Applying QoS policies to authenticated users through user profiles

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

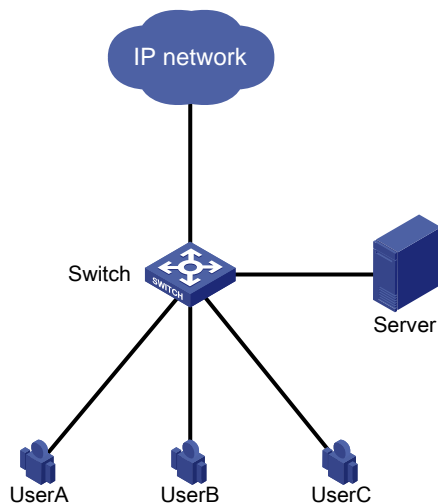
### Network requirements

As shown in [Figure 182](#), the switch connects to three 802.1X users through different ports. The users might move to other ports.

Configure traffic control to meet the following requirements:

- Limit the maximum upload rate to 1 M for User A after User A passes authentication.
- Do not allow User B to access the network from 8:30 to 12:00 every day, regardless of whether User B passes authentication.
- Set the 802.1p priority to 5 for the traffic from User C.

**Figure 182 Network diagram**



## Requirements analysis

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

- To allow users to move to other ports, configure user profiles and associate the user profiles with the users.
- To limit the upload rate of User A, configure traffic policing.
- To deny User B from accessing the network from 8:30 to 12:00 every day, use a time range-based ACL and a traffic filtering action.
- To mark the 802.1p priority for traffic from User C, use the priority marking function.

## Configuration restrictions and guidelines

When you apply QoS policies to authenticated users through user profiles, follow these restrictions and guidelines:

- If a user profile has been enabled, you can modify the ACL referenced by the QoS policy in the user profile. However, you cannot modify other contents of the QoS policy or delete the QoS policy. If the user associated with the user profile has been online, you also cannot modify the ACL referenced by the QoS policy.
- The traffic behaviors of a QoS policy that applies to a user profile only support the **remark**, **car**, and **filter** actions.
- A QoS policy that applies to a user profile must have contents. Otherwise, the user profile cannot be enabled.
- After you apply a QoS policy to a user profile, the QoS policy automatically adds match criteria to match the MAC address (**macbased**) or IP address (**portbased**) of users. Therefore, you only need to configure the traffic classifier to match all traffic. The same is true for User B and User C.

## Configuration procedures

### Configuring user authentication

# Configure 802.1X authentication on the switch and the authentication server. For more information, see *802.1X Configuration Examples*.

### Configuring QoS policies

1. Configure a QoS policy to limit the upload rate of User A.

# Configure a traffic classifier **for\_usera** to match all traffic.

```
<Switch> system-view
[Switch] traffic classifier for_usera
[Switch-classifier-for_usera] if-match any
[Switch-classifier-for_usera] quit
```

# Configure a traffic behavior **for\_usera** to limit the upload rate to 1 M (1024 kbps) for User A.

```
[Switch] traffic behavior for_usera
[Switch-behavior-for_usera] car cir 1024
[Switch-behavior-for_usera] quit
```

# Configure a QoS policy **for\_usera**, and associate the traffic classifier **for\_usera** with the traffic behavior **for\_usera**.

```
[Switch] qos policy for_usera
[Switch-qospolicy-for_usera] classifier for_usera behavior for_usera
[Switch-qospolicy-for_usera] quit
```

2. Configure a QoS policy to deny User B from accessing the network from 8:30 to 12:00 every day:

# Configure a time range **for\_userb** that defines 8:30 to 12:00 every day.

```
[Switch] time-range for_userb 8:30 to 12:00 daily
```

# Configure basic ACL 2000 to match all traffic within the time range **for\_userb**.

```
[Switch] acl number 2000
```

```
[Switch-acl-basic-2000] rule permit time-range for_userb
```

```
[Switch-acl-basic-2000] quit
```

# Configure a traffic classifier **for\_userb** to match the traffic permitted by ACL 2000.

```
[Switch] traffic classifier for_userb
```

```
[Switch-classifier-for_userb] if-match acl 2000
```

```
[Switch-classifier-for_userb] quit
```

# Configure a traffic behavior **for\_userb** to deny the matching traffic.

```
[Switch] traffic behavior for_userb
```

```
[Switch-behavior-for_userb] filter deny
```

```
[Switch-behavior-for_userb] quit
```

# Configure a QoS policy **for\_userb**, and associate the traffic classifier **for\_userb** with the traffic behavior **for\_userb**.

```
[Switch] qos policy for_userb
```

```
[Switch-qospolicy-for_userb] classifier for_userb behavior for_userb
```

```
[Switch-qospolicy-for_userb] quit
```

3. Configure a QoS policy to mark the 802.1p priority for traffic from User C:

# Configure a traffic classifier **for\_userc** to match all traffic.

```
[Switch] traffic classifier for_userc
```

```
[Switch-classifier-for_userc] if-match any
```

```
[Switch-classifier-for_userc] quit
```

# Configure a traffic behavior **for\_userc** to set the 802.1p priority as 5.

```
[Switch] traffic behavior for_userc
```

```
[Switch-behavior-for_userc] remark dot1p 5
```

```
[Switch-behavior-for_userc] quit
```

# Configure a QoS policy **for\_userc**, and associate the traffic classifier **for\_userc** with the traffic behavior **for\_userc**.

```
[Switch] qos policy for_userc
```

```
[Switch-qospolicy-for_userc] classifier for_userc behavior for_userc
```

```
[Switch-qospolicy-for_userc] quit
```

## Creating user profiles and applying QoS policies to user profiles

1. Create a user profile for User A:

# Create a user profile **usera**.

```
[Switch] user-profile usera
```

```
[Switch-user-profile-usera]
```

# Apply the QoS policy **for\_usera** to the user profile in the inbound direction to limit the upload rate of User A.

```
[Switch-user-profile-usera] qos apply policy for_usera inbound
```

- ```
[Switch-user-profile-usera] quit
# Enable the user profile.
[Switch] user-profile usera enable
# Configure the authentication server to assign the user profile usera after User A passes authentication. For more information, see the user manual of the authentication server.
```
2. Create a user profile for User B:
- ```
Create a user profile userb.
[Switch] user-profile userb
[Switch-user-profile-userb]
Apply the QoS policy for_userb to the user profile in the inbound direction to filter traffic from User B.
[Switch-user-profile-userb] qos apply policy for_userb inbound
[Switch-user-profile-userb] quit
Enable the user profile.
[Switch] user-profile userb enable
Configure the authentication server to assign the user profile userb after User B passes authentication.
```
3. Create a user profile for User C:
- ```
# Create a user profile userc.
[Switch] user-profile userc
[Switch-user-profile-userc]
# Apply the QoS policy for_userc to the user profile in the inbound direction to set the 802.1p priority for traffic from User C.
[Switch-user-profile-userc] qos apply policy for_userc inbound
[Switch-user-profile-userc] quit
# Enable the user profile.
[Switch] user-profile userc enable
# Configure the authentication server to assign the user profile userc after User C passes authentication.
```

Verifying the configuration

```
# Display QoS policies.
<Switch> display qos policy user-defined
```

```
User Defined QoS Policy Information:

Policy: for_usera
Classifier: for_usera
Behavior: for_usera
Committed Access Rate:
  CIR 1024 (kbps), CBS 64000 (byte), EBS 512 (byte)
Green Action: pass
Red Action: discard
Yellow Action: pass
```

```
Policy: for_userb
Classifier: for_userb
Behavior: for_userb
Filter enable: deny
```

```
Policy: for_userc
Classifier: for_userc
Behavior: for_userc
Marking:
Remark dot1p COS 5
```

Configuration files

```
#
time-range for_userb 08:30 to 12:00 daily
#
acl number 2000
rule 0 permit time-range for_userb
#
traffic classifier for_usera operator and
if-match any
traffic classifier for_userb operator and
if-match acl 2000
traffic classifier for_userc operator and
if-match any
#
traffic behavior for_usera
car cir 1024 cbs 64000 ebs 512 green pass red discard yellow pass
traffic behavior for_userb
filter deny
traffic behavior for_userc
remark dot1p 5
#
qos policy for_usera
classifier for_usera behavior for_usera
qos policy for_userb
classifier for_userb behavior for_userb
qos policy for_userc
classifier for_userc behavior for_userc
#
user-profile usera
qos apply policy for_usera inbound
user-profile userb
qos apply policy for_userb inbound
user-profile userc
qos apply policy for_userc inbound
```

Control plane protection configuration examples

This chapter provides control plane protection configuration examples.

Example: Configuring control plane protection

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

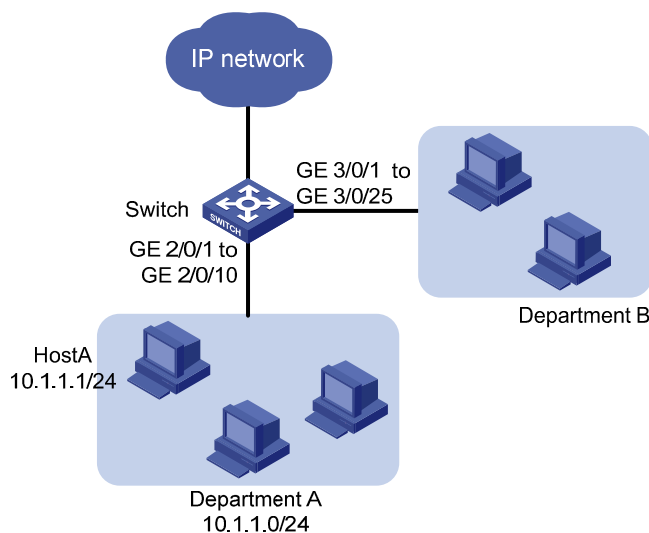
Network requirements

As shown in [Figure 183](#), Switch, which is a distributed device, uses multiple ports on different interface cards to connect the two departments of the company.

Apply a QoS policy to the control plane to protect it as follows:

- In department A, limit the rate to 64 kbps for Telnet traffic from any host except Host A to Switch.
- Perform no limit on the rate of Telnet traffic from Host A to Switch.
- Limit the rate to 192 kbps for the ARP requests from Switch to department B.
- Perform no processing for the excess ARP requests.
- Collect statistics about the processed ARP packets to avoid ARP request attacks against Switch.

Figure 183 Network diagram



Requirements analysis

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

- A QoS policy is a set of class-behavior associations that are matched in the order that they are configured. You can use this feature to configure exceptional handling (not rate limiting) for the Telnet packets from Host A.
- Because the switch has pre-defined match criteria for ARP packets, you can perform the following configurations to rate limit and collect statistics about ARP packets:
 - Use the pre-defined system index-based match criteria for ARP packets in a class.
 - Associate the class with a behavior containing a traffic policing action and traffic accounting action.

Configuration restrictions and guidelines

When you configure control plane protection, follow these restrictions and guidelines:

- In a control plane QoS policy, a class using a system index-based match criterion can be associated with only a behavior containing traffic policing, traffic accounting, or both actions. Only the CIR configured for the traffic policing action applies.
- If the QoS policy applied to a control plane does not use the system index as the match criteria, the QoS policy also takes effect on the data traffic of the card where the control plane resides.
- Because the switch does not pre-define match criteria for Telnet packets, you must configure advanced ACLs to match Telnet protocol packets.

Configuration procedures

Configuring a control plane policy for the Telnet protocol

Configure IPv4 advanced ACL 3000 to match the Telnet protocol packets sourced from Host A.

```
<Switch> system-view
[Switch] acl number 3000
[Switch-acl-adv-3000] rule permit tcp source 10.1.1.1 0 destination-port eq telnet
[Switch-acl-adv-3000] quit
```

Configure IPv4 advanced ACL 3001 to match the Telnet protocol packets sourced from network segment 10.1.1.0/24.

```
[Switch] acl number 3001
[Switch-acl-adv-3001] rule permit tcp source 10.1.1.0 0.0.0.255 destination-port eq telnet
[Switch-acl-adv-3001] quit
```

Create a class named **host_a**, and use IPv4 ACL 3000 as the match criterion.

```
[Switch] traffic classifier host_a
[Switch-classifier-host_a] if-match acl 3000
[Switch-classifier-host_a] quit
```

Create traffic behavior **host_a**, and configure an action of permitting packets to pass through in the behavior.

```
[Switch] traffic behavior host_a
[Switch-behavior-host_a] filter permit
[Switch-behavior-host_a] quit
```

Create a class named **dept_a**, and use IPv4 ACL 3001 as the match criterion.

```
[Switch] traffic classifier dept_a
[Switch-classifier-dept_a] if-match acl 3001
[Switch-classifier-dept_a] quit
```

Create a traffic behavior named **dept_a**, and configure an action of rate limiting packets to 64 kbps in the behavior.

```
[Switch] traffic behavior dept_a
[Switch-behavior-dept_a] car cir 64
[Switch-behavior-dept_a] quit
```

Create a QoS policy named **for_telnet**.

```
[Switch] qos policy for_telnet
```

Associate class **host_a** with behavior **host_a**.

```
[Switch-qospolicy-for_telnet] classifier host_a behavior host_a
```

Associate class **dept_a** with behavior **dept_a**.

```
[Switch-qospolicy-for_telnet] classifier dept_a behavior dept_a
[Switch-qospolicy-for_telnet] quit
```

Apply QoS policy **for_telnet** to the incoming traffic of the control plane of the card in slot 2.

```
[Switch] control-plane slot 2
[Switch-cp-slot2] qos apply policy for_telnet inbound
[Switch-cp-slot2] quit
```

Configuring a control plane policy for the ARP protocol

Use the **display qos policy control-plane pre-defined** command to display the pre-defined system index-based policies on the card in slot 3.

```
[Switch] display qos policy control-plane pre-defined slot 3
```

```
=====
Pre-defined Control-plane Policy Slot 3
-----
```

Index	PacketType	Priority	BandWidth(Kbps)
1	ISIS	4	256
4	VRRP	5	256
7	IPV4_MC_RIP	4	256
8	IPV4_BC_RIP	4	256
9	MCAST_NTP	3	64
10	BCAST_NTP	3	64
11	IPV4_MC OSPF_5	4	256
12	IPV4_MC OSPF_6	4	256
13	IPV4_UC OSPF	4	256
14	IPV4_MC_PIM	3	128
15	IPV4_UC_PIM	3	128
16	IPV4_IGMP	3	64
17	LDP	3	128
18	IPV6_MC_PIM	3	128
19	IPV6_UC_PIM	3	128
20	IPV6_MLD	3	64
21	IPV6_RIPNG	3	256

22	IPV6_UC_OSPFV3	3	256
23	IPV6_MC_OSPFV3_5	3	256
24	IPV6_MC_OSPFV3_6	3	256
25	IPV6_LDP	3	64
26	IPV6_VRRP	3	256
27	RRPP	6	64
28	IPV4_AUTORP	3	64
29	ARP	1	64
30	ARP_REPLY	1	64
31	DHCP_CLIENT	3	256
32	DHCP_SERVER	3	256
33	DHCP_RELAY_CLIENT	3	256
34	DHCP_RELAY_SERVER	3	256
35	DOT1X	1	64
36	STP	6	128
37	LACP	5	64
38	GVRP	3	256
39	HGMP	5	128
40	BGP	3	256
41	ICMP	1	640
44	IPV6_BGP	3	256
45	IPV6_ND_PASS	1	128
46	IPV6_ND_DEST	1	128
47	IPV6_PING	1	128
50	IPV6_DHCP	3	64
53	LLDP	3	128
54	DLDP	3	64
61	TELNET/SSH	1	512
62	HTTP/HTTPS	1	128
63	SNMP	1	512
64	SMARTLINK	6	64
67	ARP_DAI	1	128
71	IPV4_UC_DHCP	3	256
72	IPV4_UCOSPF_TTL	4	256
73	IPV4_UC_PIM_TTL	3	64
74	BGP_TTL	3	256
76	IPV6_ICMP	1	640
77	IPV6_TELNET/SSH	1	512
80	HGMP_BC	6	64
82	PVST	3	768
88	HGMP_BRIDGEMAC	6	256
90	DHCPV6_UC_CLIENT	3	256
91	DHCPV6_UC_RELAY	3	256
92	DHCPV6_RSERVER	3	256
94	BFD_ARP_REPLY	2	256
98	BFD_ECHO	5	256
99	BFD_CTRL	5	256
100	BFD_MULTIHOP	5	256

102	IPV6_ND_DAI	3	128
103	IPV6_DHCP_CLIENT	3	256
104	IPV6_DHCP_SERVER	3	256
105	IRDP	4	256
106	IPV6_CPU_DST_CAR	3	128

=====
The output shows that the system-index for ARP request is 29, and the pre-defined rate limit is 64 kbps.

NOTE:

The pre-defined system indexes for protocols vary by device model and software version. Make the following configurations based on the pre-defined system indexes on your switch.

Create a class named **for_arp**, and use system index 29 as the match criterion.

```
[Switch] traffic classifier for_arp
[Switch-classifier-for_arp] if-match system-index 29
[Switch-classifier-for_arp] quit
```

Create a traffic behavior named **for_arp**, and configure an action of rate limiting packets to 192 kbps and a traffic accounting action in the behavior.

```
[Switch] traffic behavior for_arp
[Switch-behavior-for_arp] car cir 192
[Switch-behavior-for_arp] accounting
[Switch-behavior-for_arp] quit
```

Create a QoS policy named **for_arp**, and associate class **for_arp** with traffic behavior **for_arp** in the QoS policy.

```
[Switch] qos policy for_arp
[Switch-qospolicy-for_arp] classifier for_arp behavior for_arp
[Switch-qospolicy-for_arp] quit
```

Apply QoS policy **for_arp** to the incoming traffic of the control plane of the card in slot 3.

```
[Switch] control-plane slot 3
[Switch-cp-slot3] qos apply policy for_arp inbound
[Switch-cp-slot3] quit
```

Verifying the configuration

Display the control plane QoS policy information on the card in slot 2.

```
[Switch] display qos policy control-plane slot 2
Control-plane slot 2
  Direction: Inbound
  Policy: for_telnet
  Classifier: host_a
    Operator: AND
    Rule(s) : If-match acl 3000
  Behavior: host_a
    Filter Enable: permit
  Classifier: dept_a
    Operator: AND
    Rule(s) : If-match acl 3001
```

```

Behavior: dept_a
Committed Access Rate:
  CIR 64 (Kbps), CBS 512 (byte), EBS 512 (byte)
  Green Action: pass
  Red Action: discard
  Yellow Action: pass
  Green : 0(Packets)
  Red   : 0(Packets)

```

Display the pre-defined control plane QoS policy information on the card in slot 3.

```
[Switch] display qos policy control-plane pre-defined slot 3
```

```
<Sysname> display qos policy control-plane pre-defined slot 2
```

```

=====
Pre-defined Control-plane Policy Slot 2
-----

```

Index	PacketType	Priority	BandWidth(Kbps)
1	ISIS	4	256
4	VRRP	5	256
7	IPV4_MC_RIP	4	256
8	IPV4_BC_RIP	4	256
9	MCAST_NTP	3	64
10	BCAST_NTP	3	64
11	IPV4_MC_OSPF_5	4	256
12	IPV4_MC_OSPF_6	4	256
13	IPV4_UC_OSPF	4	256
14	IPV4_MC_PIM	3	128
15	IPV4_UC_PIM	3	128
16	IPV4_IGMP	3	64
17	LDP	3	128
18	IPV6_MC_PIM	3	128
19	IPV6_UC_PIM	3	128
20	IPV6_MLD	3	64
21	IPV6_RIPNG	3	256
22	IPV6_UC_OSPFV3	3	256
23	IPV6_MC_OSPFV3_5	3	256
24	IPV6_MC_OSPFV3_6	3	256
25	IPV6_LDP	3	64
26	IPV6_VRRP	3	256
27	RRPP	6	64
28	IPV4_AUTORP	3	64
29	ARP	1	192
30	ARP_REPLY	1	64
31	DHCP_CLIENT	3	256
32	DHCP_SERVER	3	256
33	DHCP_RELAY_CLIENT	3	256
34	DHCP_RELAY_SERVER	3	256
35	DOT1X	1	64
36	STP	6	128

37	LACP	5	64
38	GVRP	3	256
39	HGMP	5	128
40	BGP	3	256
41	ICMP	1	640
44	IPV6_BGP	3	256
45	IPV6_ND_PASS	1	128
46	IPV6_ND_DEST	1	128
47	IPV6_PING	1	128
50	IPV6_DHCP	3	64
53	LLDP	3	128
54	DLDP	3	64
61	TELNET/SSH	1	512
62	HTTP/HTTPS	1	128
63	SNMP	1	512
64	SMARTLINK	6	64
67	ARP_DAI	1	128
71	IPV4_UC_DHCP	3	256
72	IPV4_UCOSPF_TTL	4	256
73	IPV4_UC_PIM_TTL	3	64
74	BGP_TTL	3	256
76	IPV6_ICMP	1	640
77	IPV6_TELNET/SSH	1	512
80	HGMP_BC	6	64
82	PVST	3	768
88	HGMP_BRIDGEMAC	6	256
90	DHCPV6_UC_CLIENT	3	256
91	DHCPV6_UC_RELAY	3	256
92	DHCPV6_RSERVER	3	256
94	BFD_ARP_REPLY	2	256
98	BFD_ECHO	5	256
99	BFD_CTRL	5	256
100	BFD_MULTIHOP	5	256
102	IPV6_ND_DAI	3	128
103	IPV6_DHCP_CLIENT	3	256
104	IPV6_DHCP_SERVER	3	256
105	IRDP	4	256
106	IPV6_CPUDST_CAR	3	128

=====

The output shows the rate limit for ARP protocol packets becomes the user-defined 192 kbps.

Configuration files

```
#
acl number 3000
 rule 0 permit tcp source 10.1.1.1 0 destination-port eq telnet
acl number 3001
 rule 0 permit tcp source 10.1.1.0 0.0.0.255 destination-port eq telnet
```

```
#
traffic classifier host_a operator and
  if-match acl 3000
traffic classifier for_arp operator and
  if-match system-index 29
traffic classifier dept_a operator and
  if-match acl 3001
#
traffic behavior host_a
  filter permit
traffic behavior for_arp
  car cir 192 cbs 512 ebs 512 green pass red discard yellow pass
  accounting
traffic behavior dept_a
  car cir 64 cbs 512 ebs 512 green pass red discard yellow pass
#
qos policy for_telnet
  classifier host_a behavior host_a
  classifier dept_a behavior dept_a
qos policy for_arp
  classifier for_arp behavior for_arp
#
control-plane slot 2
  qos apply policy for_telnet inbound
control-plane slot 3
  qos apply policy for_arp inbound
```

QoS policy-based routing configuration examples

This chapter provides QoS policy-based routing configuration examples.

Example: Configuring QoS policy-based IPv4 routing

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

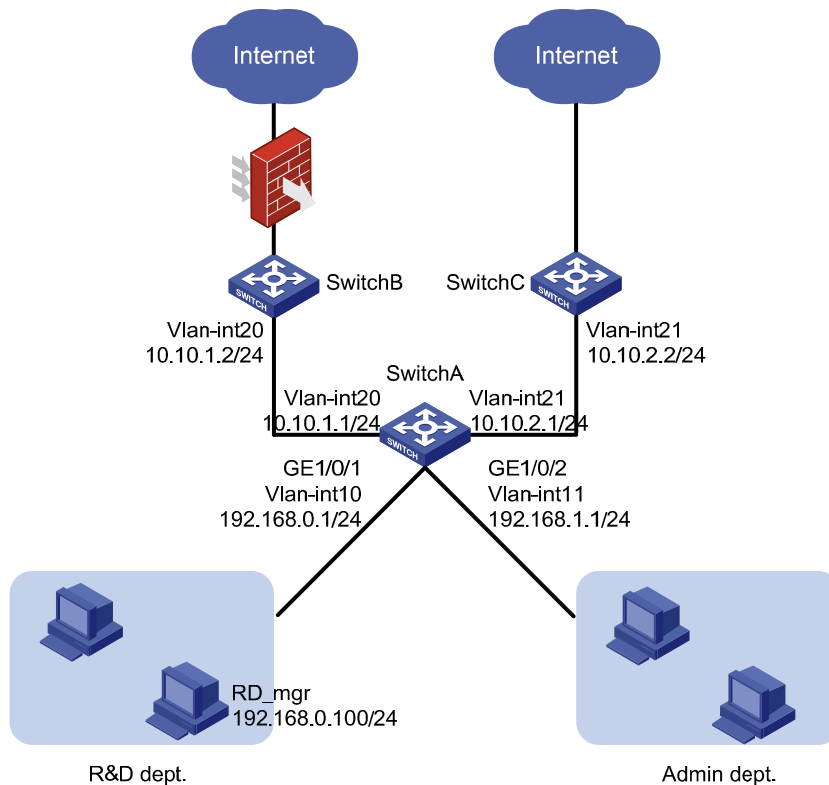
Network requirements

As shown in [Figure 184](#), a company accesses the Internet through two SP networks. The Administration department and the R&D department of the company need to access the Internet.

Configure QoS policy-based IPv4 routing to meet the following requirements:

- The R&D department accesses the specified websites in the Internet through the uplink of Switch B. The firewall filters and logs the website access.
The Administration department can access the Internet through Switch C without any restrictions.
- The host of the R&D department manager, with the IP address 192.168.0.100, can access the Internet through Switch C without any restrictions.

Figure 184 Network diagram



Requirements analysis

To allow packets with specific source IP addresses to be forwarded along specified paths, configure a QoS policy to redirect the packets to specified next hops.

Configuration restrictions and guidelines

When you configure QoS policy-based IPv4 routing, follow these restrictions and guidelines:

- Before you configure QoS policy-based routing, make sure all devices can reach each other through traditional routing protocols.
- You must configure the class-behavior association for the R&D department manager before you configure the class-behavior association for the entire network segment of the R&D department. Otherwise, the configuration for the R&D department manager fails.

Configuration procedures

Configuring routing protocols

Configure VLAN-interfaces and assign IP addresses to VLAN-interfaces on these devices, as shown in Figure 184. (Details not shown.)

Configure OSPF on Switch A to advertise the directly connected networks of Switch A.

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.10.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.10.2.0 0.0.0.255
```

Configure OSPF on Switch B to advertise the directly connected networks of Switch B.

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.10.1.0 0.0.0.255
```

Configure OSPF on Switch C to advertise the directly connected networks of Switch C.

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.10.2.0 0.0.0.255
```

Perform the following configurations:

- Configure the default gateway address as 192.168.0.1 for the hosts of the R&D department.
- Configure the default gateway address as 192.168.1.1 for the hosts in the Administration department.

After completing the configuration, check whether each department can reach Switch B and Switch C. If they can, the routing protocols are correctly configured, and you can proceed with the following configurations.

Configuring QoS policy-based routing

Configure basic ACL 2000 to match the traffic with source IP address 192.168.0.0/24.

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 192.168.0.0 0.0.0.255
[SwitchA-acl-basic-2000] quit
```

Configure basic ACL 2001 to match the traffic with source IP address 192.168.1.0/24.

```
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 192.168.1.0 0.0.0.255
[SwitchA-acl-basic-2001] quit
```

Configure basic ACL 2002 to match the traffic with source IP address 192.168.0.100 (IP address of the R&D department manager's host).

```
[SwitchA] acl number 2002
[SwitchA-acl-basic-2002] rule permit source 192.168.0.100 0.0.0.0
[SwitchA-acl-basic-2002] quit
```

Create class **rd_internet**, and use ACL 2000 as the match criterion of the class.

```
[SwitchA] traffic classifier rd_internet
[SwitchA-classifier-rd_internet] if-match acl 2000
```

```

[SwitchA-classifier-rd_internet] quit

# Create a behavior named rd_internet, and configure the action of redirecting traffic to Switch B
(10.10.1.2) for the behavior.
[SwitchA] traffic behavior rd_internet
[SwitchA-behavior-rd_internet] redirect next-hop 10.10.1.2
[SwitchA-behavior-rd_internet] quit

# Create class admin_internet, and use ACL 2001 as the match criterion of the class.
[SwitchA] traffic classifier admin_internet
[SwitchA-classifier-admin_internet] if-match acl 2001
[SwitchA-classifier-admin_internet] quit

# Create a behavior named admin_internet, and configure the action of redirecting traffic to Switch C
(10.10.2.2) for the behavior.
[SwitchA] traffic behavior admin_internet
[SwitchA-behavior-admin_internet] redirect next-hop 10.10.2.2
[SwitchA-behavior-admin_internet] quit

# Create class rd_mgr_internet, and use ACL 2002 as the match criterion of the class.
[SwitchA] traffic classifier rd_mgr_internet
[SwitchA-classifier-rd_mgr_internet] if-match acl 2002
[SwitchA-classifier-rd_mgr_internet] quit

# Create a QoS policy named rd_internet.
[SwitchA] qos policy rd_internet

# Associate class rd_mgr_internet with traffic behavior admin_internet.
[SwitchA-qospolicy-rd_internet] classifier rd_mgr_internet behavior admin_internet

# Associate class rd_internet with traffic behavior rd_internet.
[SwitchA-qospolicy-rd_internet] classifier rd_internet behavior rd_internet
[SwitchA-qospolicy-rd_internet] quit

# Create a QoS policy named admin_internet, and associate class admin_internet with traffic behavior
admin_internet.
[SwitchA] qos policy admin_internet
[SwitchA-qospolicy-admin_internet] classifier admin_internet behavior admin_internet
[SwitchA-qospolicy-admin_internet] quit

# Apply the QoS policy rd_internet to the incoming traffic of GigabitEthernet 1/0/1.
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos apply policy rd_internet inbound
[SwitchA-GigabitEthernet1/0/1] quit

# Apply the QoS policy admin_internet to the incoming traffic of GigabitEthernet 1/0/2.
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] qos apply policy admin_internet inbound
[SwitchA-GigabitEthernet1/0/2] quit

```

Verifying the configuration

```
# Display information about QoS policies applied to ports.
```

```
[SwitchA] display qos policy interface
```

```
Interface: GigabitEthernet1/2/0/2
```

```
Direction: Inbound
```

```
Policy: rd_internet
```

```
Classifier: rd_mgr_internet
```

```
Operator: AND
```

```
Rule(s) : If-match acl 2002
```

```
Behavior: admin_internet
```

```
Redirect enable:
```

```
Redirect type: next-hop
```

```
Redirect destination:
```

```
10.10.2.2
```

```
Redirect fail-action: forward
```

```
Classifier: rd_internet
```

```
Operator: AND
```

```
Rule(s) : If-match acl 2000
```

```
Behavior: rd_internet
```

```
Redirect enable:
```

```
Redirect type: next-hop
```

```
Redirect destination:
```

```
10.10.1.2
```

```
Redirect fail-action: forward
```

```
Interface: GigabitEthernet1/2/0/3
```

```
Direction: Inbound
```

```
Policy: admin_internet
```

```
Classifier: admin_internet
```

```
Operator: AND
```

```
Rule(s) : If-match acl 2001
```

```
Behavior: admin_internet
```

```
Redirect enable:
```

```
Redirect type: next-hop
```

```
Redirect destination:
```

```
10.10.2.2
```

```
Redirect fail-action: forward
```

Configuration files

This section provides only the configuration files on Switch A. Only routing protocols need to be configured on Switch B and Switch C. Their configuration files are not provided.

```
#
acl number 2000
  rule 0 permit source 192.168.0.0 0.0.0.255
acl number 2001
  rule 0 permit source 192.168.1.0 0.0.0.255
acl number 2002
  rule 0 permit source 192.168.0.100 0
#
traffic classifier admin_internet operator and
  if-match acl 2001
traffic classifier rd_mgr_internet operator and
  if-match acl 2002
traffic classifier rd_internet operator and
  if-match acl 2000
#
traffic behavior admin_internet
  redirect next-hop 10.10.2.2 fail-action forward
traffic behavior rd_internet
  redirect next-hop 10.10.1.2 fail-action forward
#
qos policy admin_internet
  classifier admin_internet behavior admin_internet
qos policy rd_internet
  classifier rd_mgr_internet behavior admin_internet
  classifier rd_internet behavior rd_internet
#
interface GigabitEthernet1/0/1
  qos apply policy rd_internet inbound
#
interface GigabitEthernet1/0/2
  qos apply policy admin_internet inbound
#
ospf 1
  area 0.0.0.0
    network 192.168.0.0 0.0.0.255
    network 192.168.1.0 0.0.0.255
    network 10.1.1.0 0.0.0.255
    network 10.1.2.0 0.0.0.255
```

Example: Configuring QoS policy-based IPv6 routing

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

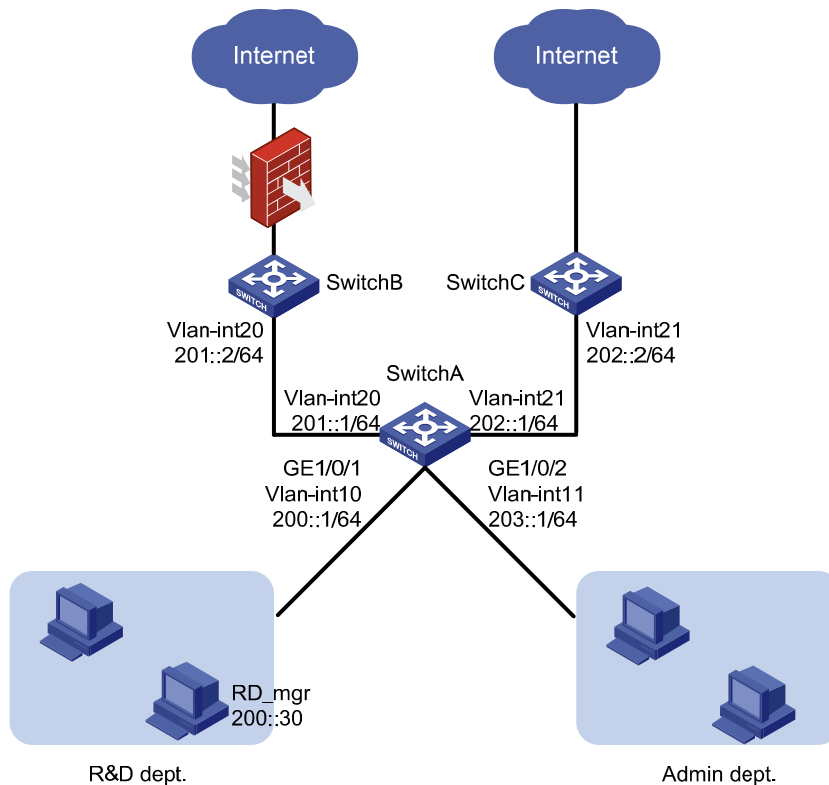
Network requirements

As shown in [Figure 185](#), a company accesses the Internet through two SP networks. The Administration department and the R&D department of the company need to access the Internet.

Configure QoS policy-based IPv6 routing to meet the following requirements:

- The R&D department accesses the specified websites in the Internet through the uplink of Switch B. The firewall filters and logs the website access.
- The Administration department can access the Internet through Switch C without any restrictions.
- The host of the R&D department manager, with the IPv6 address 200::30, can access the Internet through Switch C without any restrictions.

Figure 185 Network diagram



Requirements analysis

To allow packets with specific source IPv6 addresses to be forwarded along specified paths, configure a QoS policy to redirect the packets to specified next hops.

Configuration restrictions and guidelines

When you configure QoS policy-based IPv6 routing, follow these restrictions and guidelines:

- Before you configure QoS policy-based routing, make sure all devices can reach each other through traditional routing protocols.
- You must configure the class-behavior association for the R&D department manager before you configure the class-behavior association for the entire network segment of the R&D department. Otherwise, the configuration for the R&D department manager fails.

Configuration procedures

Configuring routing protocols

Configure VLAN interfaces and assign IP addresses to VLAN-interfaces on these devices, as shown in Figure 185. (Details not shown.)

Enable RIPng on Switch A, and enable RIPng on each VLAN interface on Switch A.

```
<SwitchA> system-view
[SwitchA] ripng
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ripng 1 enable
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ripng 1 enable
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ripng 1 enable
[SwitchA] interface vlan-interface 21
[SwitchA-Vlan-interface21] ripng 1 enable
```

Enable RIPng on Switch B, and enable RIPng on VLAN-interface 20.

```
<SwitchB> system-view
[SwitchB] ripng
[SwitchB-ripng-1] quit
[SwitchB] interface vlan-interface 20
[SwitchB-Vlan-interface20] ripng 1 enable
```

Enable RIPng on Switch C, and enable RIPng on VLAN-interface 21.

```
<SwitchC> system-view
[SwitchC] ripng
[SwitchC-ripng-1] quit
[SwitchC] interface vlan-interface 21
[SwitchC-Vlan-interface21] ripng 1 enable
```

Perform the following configurations:

- Configure the default gateway address as 200::1/64 for the hosts of the R&D department.
- Configure the default gateway address as 203::1/64 for the hosts in the Administration department.

After completing the configuration, check whether each department can reach Switch B and Switch C. If they can, the routing protocols are correctly configured, and you can proceed with the following configurations.

Configuring QoS policy-based routing

Configure IPv6 basic ACL 2000 to match the traffic with source IP address 200::0/64.

```
[SwitchA] acl ipv6 number 2000
[SwitchA-acl6-basic-2000] rule permit source 200::0 64
[SwitchA-acl6-basic-2000] quit
```

Configure IPv6 basic ACL 2001 to match the traffic with source IP address 203::0/64.

```
[SwitchA] acl ipv6 number 2001
[SwitchA-acl6-basic-2001] rule permit source 203::0 64
[SwitchA-acl6-basic-2001] quit
```

Configure IPv6 basic ACL 2002 to match the traffic with source IP address 200::30/128 (IP address of the R&D department manager's host).

```
[SwitchA] acl ipv6 number 2002
```



```

[SwitchA-acl6-basic-2002] rule permit source 200::30 128
[SwitchA-acl6-basic-2002] quit

# Create class rd_internet, and use IPv6 ACL 2000 as the match criterion of the class.
[SwitchA] traffic classifier rd_internet
[SwitchA-classifier-rd_internet] if-match acl ipv6 2000
[SwitchA-classifier-rd_internet] quit

# Create a behavior named rd_internet, and configure the action of redirecting traffic to Switch B (201::2)
for the behavior.
[SwitchA] traffic behavior rd_internet
[SwitchA-behavior-rd_internet] redirect next-hop 201::2
[SwitchA-behavior-rd_internet] quit

# Create class admin_internet, and use IPv6 ACL 2001 as the match criterion of the class.
[SwitchA] traffic classifier admin_internet
[SwitchA-classifier-admin_internet] if-match acl ipv6 2001
[SwitchA-classifier-admin_internet] quit

# Create a behavior named admin_internet, and configure the action of redirecting traffic to Switch C
(202::2) for the behavior.
[SwitchA] traffic behavior admin_internet
[SwitchA-behavior-admin_internet] redirect next-hop 202::2
[SwitchA-behavior-admin_internet] quit

# Create class rd_mgr_internet, and use IPv6 ACL 2002 as the match criterion of the class.
[SwitchA] traffic classifier rd_mgr_internet
[SwitchA-classifier-rd_mgr_internet] if-match acl ipv6 2002
[SwitchA-classifier-rd_mgr_internet] quit

# Create a QoS policy named rd_internet.
[SwitchA] qos policy rd_internet

# Associate class rd_mgr_internet with traffic behavior admin_internet.
[SwitchA-qospolicy-rd_internet] classifier rd_mgr_internet behavior admin_internet

# Associate class rd_internet with traffic behavior rd_internet.
[SwitchA-qospolicy-rd_internet] classifier rd_internet behavior rd_internet
[SwitchA-qospolicy-rd_internet] quit

# Create a QoS policy named admin_internet, and associate class admin_internet with traffic behavior
admin_internet.
[SwitchA] qos policy admin_internet
[SwitchA-qospolicy-admin_internet] classifier admin_internet behavior admin_internet
[SwitchA-qospolicy-admin_internet] quit

# Apply the QoS policy rd_internet to the incoming traffic of GigabitEthernet 1/0/1.
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos apply policy rd_internet inbound
[SwitchA-GigabitEthernet1/0/1] quit

# Apply the QoS policy admin_internet to the incoming traffic of GigabitEthernet 1/0/2.
[SwitchA] interface gigabitethernet 1/0/2

```

```
[SwitchA-GigabitEthernet1/0/2] qos apply policy admin_internet inbound
[SwitchA-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Display information about QoS policies applied to ports.

```
[SwitchA] display qos policy interface
```

```
Interface: GigabitEthernet1/0/1
```

```
Direction: Inbound
```

```
Policy: admin_internet
```

```
Classifier: admin_internet
```

```
Operator: AND
```

```
Rule(s) : If-match acl 2001
```

```
          If-match acl ipv6 2001
```

```
Behavior: admin_internet
```

```
Redirect enable:
```

```
Redirect type: next-hop
```

```
Redirect destination:
```

```
202::2
```

```
Redirect fail-action: forward
```

```
Interface: GigabitEthernet1/0/2
```

```
Direction: Inbound
```

```
Policy: admin_internet
```

```
Classifier: admin_internet
```

```
Operator: AND
```

```
Rule(s) : If-match acl 2001
```

```
          If-match acl ipv6 2001
```

```
Behavior: admin_internet
```

```
Redirect enable:
```

```
Redirect type: next-hop
```

```
Redirect destination:
```

```
202::2
```

```
Redirect fail-action: forward
```

Configuration files

```
#
acl ipv6 number 2000
 rule 0 permit source 200::/64
acl ipv6 number 2001
 rule 0 permit source 203::/64
```

```

acl ipv6 number 2002
  rule 0 permit source 200::30/128
#
traffic classifier admin_internet operator and
  if-match acl ipv6 2001
traffic classifier rd_mgr_internet operator and
  if-match acl ipv6 2002
traffic classifier rd_internet operator and
  if-match acl ipv6 2000
#
traffic behavior admin_internet
  redirect next-hop 202::2 fail-action forward
traffic behavior rd_internet
  redirect next-hop 201::2 fail-action forward
#
qos policy admin_internet
  classifier admin_internet behavior admin_internet
qos policy rd_internet
  classifier rd_mgr_internet behavior admin_internet
  classifier rd_internet behavior rd_internet
#
interface Vlan-interface10
  ripng 1 enable
#
interface Vlan-interface11
  ripng 1 enable
#
interface Vlan-interface20
  ripng 1 enable
#
interface Vlan-interface21
  ripng 1 enable
#
interface GigabitEthernet1/0/1
  qos apply policy rd_internet inbound
#
interface GigabitEthernet1/0/2
  qos apply policy admin_internet inbound
#
ripng 1
#

```

RRPP configuration examples

This chapter provides RRPP configuration examples.

RRPP can prevent broadcast storms caused by data loops when an Ethernet ring is healthy, and rapidly restore the communication paths between the nodes in the event that a link is disconnected on the ring.

General configuration restrictions and guidelines

When you configure RRPP, follow these restrictions and guidelines:

- Do not enable OAM remote loopback function on an RRPP port. Otherwise, it may cause temporary broadcast storms.
- To ensure proper forwarding of RRPPDUs, do not enable 802.1Q in 802.1Q (QinQ) or VLAN mapping on the control VLANs.
- RRPP ports must be Layer-2 Ethernet ports or Layer-2 aggregate interfaces. The Layer-2 Ethernet ports cannot be member ports of any Layer-2 aggregation group, service loopback group, or smart link group.
- You must disable the spanning tree feature on the ports accessing an RRPP ring. Do not enable Smart Link on the ports.
- Do not configure a port accessing an RRPP ring as the monitor port of a mirroring group.
- To accelerate topology convergence, HP recommends cancelling the physical state change suppression interval setting on a port that accesses an RRPP ring.

Example: Configuring single ring

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

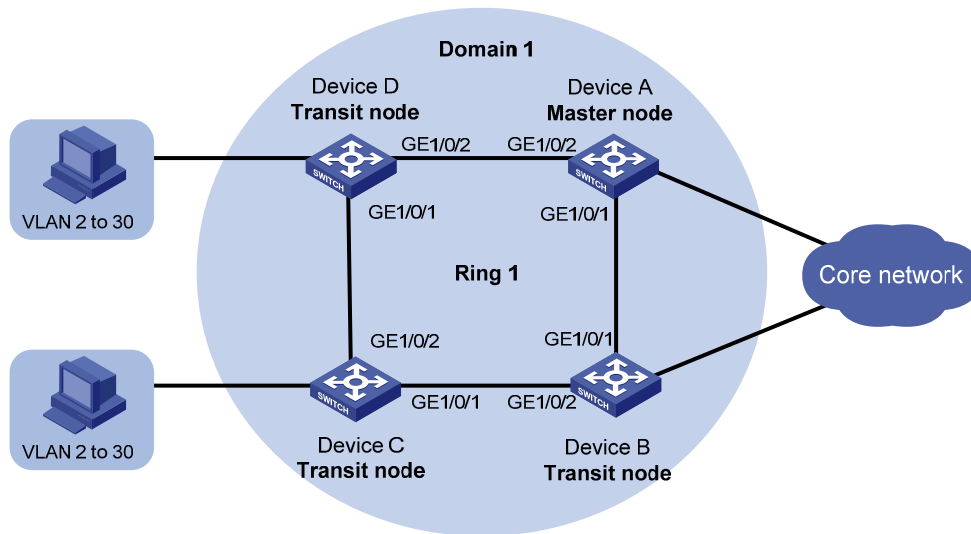
Network requirements

As shown in [Figure 186](#), multiple users are connected to the distribution-layer network that adopts an RRPP ring topology.

Configure RRPP to meet the following requirements:

- When all physical links on Ring 1 are connected:
 - The nodes on the ring can communicate with each another.
 - No broadcast storms can occur due to data loops.
- When a physical link on Ring 1 is broken, RRPP immediately restores communication between the nodes to ensure convergence performance of the network.
- When the broken link is restored, the link can forward data traffic again, and no loops occur.

Figure 186 Network diagram



Requirements analysis

The master node initiates the polling mechanism and determines the operations to be performed after a change in topology. Therefore, you must configure a device with high performance as the master node. In this example, configure Device A as the master node.

Configuration restrictions and guidelines

When you configure single ring, follow these restrictions and guidelines:

- To avoid loops caused by disabling STP, perform full-mesh connection in the ring network after you complete RRPP configurations on all devices of the ring network.
- To activate an RRPP domain on the current device, enable the RRPP protocol and RRPP rings for the RRPP domain on the current device.
- For the HP 5500 EI & HP 5500 SI Switch Series, execute the **qos trust dot1p** command in Ethernet interface view to configure the 802.1p priority of trusted packets on RRPP ports. RRPP packets then take higher precedence than data packets when passing through the RRPP ports.

Configuration procedures

Configuring Device A

Create VLANs 2 through 30.

```
<DeviceA> system-view
[DeviceA] vlan 2 to 30
Please wait... Done.
```

Map these VLANs to MSTI 1.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 2 to 30
```

Activate the MST region configuration.

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

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

Set the trusted packet priority type to 802.1p priority on the port.

```
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p
```

Configure the port as a trunk port.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 2 through 30.

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceA] rrpp domain 1
Info: Create a new domain.
```

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceA-rrpp-domain1] control-vlan 4092
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit

# Enable RRPP.
[DeviceA] rrpp enable
```

Configuring Device B

Create VLANs 2 through 30.

```
<DeviceB> system-view
[DeviceB] vlan 2 to 30
Please wait... Done.
```

Map these VLANs to MSTI 1.

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 2 to 30
```

Activate the MST region configuration.

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

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

Set the trusted packet priority type to 802.1p priority on the port.

```
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p
```

Configure the port as a trunk port.

```
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 2 through 30.

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceB-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceB] rrpp domain 1
Info: Create a new domain.
```

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceB-rrpp-domain1] control-vlan 4092
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device B as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary
port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
[DeviceB-rrpp-domain1] quit

# Enable RRPP.
[DeviceB] rrpp enable
```

Configuring Device C and Device D

Configure Device C and Device D in the same way Device B is configured. (Details not shown.)

Verifying the configuration

When all physical links on Ring 1 are connected, display detailed RRPP information about Ring 1.

```
<DeviceA> display rrpp verbose domain 1 ring 1
Domain ID      : 1
Control VLAN   : Major 4092    Sub 4093
Protected VLAN: Reference Instance 1
Hello Timer    : 1 sec  Fail Timer : 3 sec
Ring ID        : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Complete
Enable Status  : Yes    Active Status: Yes
Primary port   : GE1/0/1          Port status: UP
Secondary port : GE1/0/2          Port status: BLOCKED
```

The output shows that all physical links on Ring 1 are connected. Interface GigabitEthernet 1/0/2 on Device A is blocked and cannot forward data packets.

Shut down GigabitEthernet 1/0/2 on Device B. Display detailed RRPP information about Ring 1 on Device A and Device B.

```
<DeviceA> display rrpp verbose domain 1 ring 1
Domain ID      : 1
Control VLAN   : Major 4092    Sub 4093
Protected VLAN: Reference Instance 1
Hello Timer    : 1 sec  Fail Timer : 3 sec
Ring ID        : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Failed
Enable Status  : Yes    Active Status: Yes
Primary port   : GE1/0/1          Port status: UP
Secondary port : GE1/0/2          Port status: UP
```


The output shows that a physical link on Ring 1 is broken. Interface GigabitEthernet 1/0/2 on Device A is up and can forward data packets.

```
<DeviceB> display rrpp verbose domain 1 ring 1
Domain ID      : 1
Control VLAN   : Major 4092    Sub 4093
Protected VLAN: Reference Instance 1
Hello Timer    : 1 sec  Fail Timer : 3 sec
Ring ID       : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : -
Enable Status : Yes    Active Status: Yes
Primary port  : GE1/0/1          Port status: UP
Secondary port: GE1/0/2          Port status: Down
```

The output shows that interface GigabitEthernet 1/0/2 on Device B is down.

Bring up GigabitEthernet 1/0/2 on Device B. Display detailed RRPP information about Ring 1 on Device A and Device B.

```
<DeviceA> display rrpp verbose domain 1 ring 1
Domain ID      : 1
Control VLAN   : Major 4092    Sub 4093
Protected VLAN: Reference Instance 1
Hello Timer    : 1 sec  Fail Timer : 3 sec
Ring ID       : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Enable Status : Yes    Active Status: Yes
Primary port  : GE1/0/1          Port status: UP
Secondary port: GE1/0/2          Port status: BLOCKED
```

The output shows that all physical links on Ring 1 are connected. Interface GigabitEthernet 1/0/2 on Device A is blocked and cannot forward data packets.

```
<DeviceB> display rrpp verbose domain 1 ring 1
Domain ID      : 1
Control VLAN   : Major 4092    Sub 4093
Protected VLAN: Reference Instance 1
Hello Timer    : 1 sec  Fail Timer : 3 sec
Ring ID       : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : -
Enable Status : Yes    Active Status: Yes
Primary port  : GE1/0/1          Port status: UP
Secondary port: GE1/0/2          Port status: UP
```

The output shows that interface GigabitEthernet 1/0/2 on Device B comes up again and can forward data packets.

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp enable
#
```

- Device B, Device C, and Device D:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
```

```

stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
rrpp domain 1
control-vlan 4092
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
ring 1 enable
#
rrpp enable
#

```

Example: Configuring intersecting ring

Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

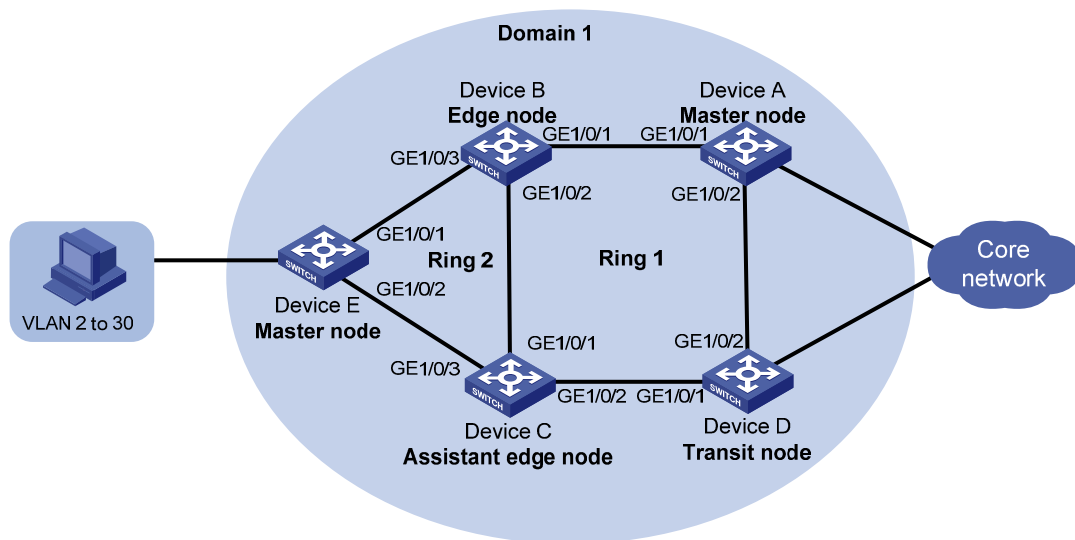
Network requirements

As shown in [Figure 187](#), Device E at the access layer is connected to the distribution layer by using a ring topology. The distribution layer also adopts a ring topology.

Configure RRPP to meet the following requirements:

- When all physical links on Ring 1 or Ring 2 are connected:
 - The nodes on the ring can communicate with each another.
 - No broadcast storms can occur due to data loops.
- When a physical link on Ring 1 or Ring 2 is broken, RRPP immediately restores communication between the nodes to ensure convergence performance of the network.
- When the broken link is restored, the link can forward data traffic again, and no loops occur.

Figure 187 Network diagram



Requirements analysis

The primary ring must feature high transmission capability for transparently transmitting traffic of the protected VLANs and control VLANs of the subrings. In this example:

- Configure Ring 1 as the primary ring.
- Configure Ring 2 as the subring.

For the primary ring, configure a device with high performance as the master node. For the subring, configure a device other than a common node as the master node. In this example:

- Configure Device A as the master node of Ring 1.
- Configure Device B as the master node of Ring 2.

Configuration restrictions and guidelines

When you configure intersecting ring, follow these restrictions and guidelines:

- To avoid loops caused by disabling STP, perform full-mesh connection in the ring network after you complete RRPP configurations on all devices of the ring network.
- To activate an RRPP domain on the current device, enable the RRPP protocol and RRPP rings for the RRPP domain on the current device.
- To prevent Hello packets of subrings from being looped on the primary ring, enable the primary ring on its master node before you enable the subrings on their separate master nodes. On an edge node or assistant-edge node, enable the primary ring of an RRPP domain before you enable the subrings of the RRPP domain.

- For the HP 5500 EI & HP 5500 SI Switch Series, execute the **qos trust dot1p** command in Ethernet interface view to configure the 802.1p priority of trusted packets on RRPP ports. RRPP packets then take higher precedence than data packets when passing through the RRPP ports.

Configuration procedures

Configuring Device A

Create VLANs 2 through 30.

```
<DeviceA> system-view
[DeviceA] vlan 2 to 30
Please wait... Done.
```

Map these VLANs to MSTI 1.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 2 to 30
```

Activate the MST region configuration.

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

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

Set the trusted packet priority type to 802.1p priority on the port.

```
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p
```

Configure the port as a trunk port.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 2 through 30.

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceA] rrpp domain 1
Info: Create a new domain.
```

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceA-rrpp-domain1] control-vlan 4092
```

```

# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary
port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit

# Enable RRPP.
[DeviceA] rrpp enable

```

Configuring Device B

```

# Create VLANs 2 through 30.
<DeviceB> system-view
[DeviceB] vlan 2 to 30
Please wait... Done.

# Map these VLANs to MSTI 1.
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 2 to 30

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

# Disable the spanning tree feature on GigabitEthernet 1/0/1.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo stp enable

# Set the trusted packet priority type to 802.1p priority on the port.
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p

# Configure the port as a trunk port.
[DeviceB-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 2 through 30.
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceB-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2.
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceB-GigabitEthernet1/0/2] quit

# Configure GigabitEthernet 1/0/3.
[DeviceB] interface gigabitethernet 1/0/3

```

```

[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] qos trust dot1p
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceB-GigabitEthernet1/0/3] quit

# Create RRPP domain 1.
[DeviceB] rrpp domain 1
Info: Create a new domain.

# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceB-rrpp-domain1] control-vlan 4092

# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device B as a transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary
port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable

# Configure Device B as the edge node of subring 2, with GigabitEthernet 1/0/3 as the edge port.
Enable ring 2.
[DeviceB-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceB-rrpp-domain1] ring 2 enable
[DeviceB-rrpp-domain1] quit

# Enable RRPP.
[DeviceB] rrpp enable

```

Configuring Device C

```

# Create VLANs 2 through 30.
<DeviceC> system-view
[DeviceC] vlan 2 to 30
Please wait... Done.

# Map these VLANs to MSTI 1.
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 2 to 30

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

# Disable the spanning tree feature on GigabitEthernet 1/0/1.
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo stp enable

# Set the trusted packet priority type to 802.1p priority on the port.
[DeviceC-GigabitEthernet1/0/1] qos trust dot1p

```

```

# Configure the port as a trunk port.
[DeviceC-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 2 through 30.
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceC-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2.
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] qos trust dot1p
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceC-GigabitEthernet1/0/2] quit

# Configure GigabitEthernet 1/0/3.
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] qos trust dot1p
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceC-GigabitEthernet1/0/3] quit

# Create RRPP domain 1.
[DeviceC] rrpp domain 1
Info: Create a new domain.

# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceC-rrpp-domain1] control-vlan 4092

# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device C as a transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary
port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable

# Configure Device C as the assistant-edge node of subring 2, with GigabitEthernet 1/0/3 as the edge
port. Enable ring 2.
[DeviceC-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain1] ring 2 enable
[DeviceC-rrpp-domain1] quit

# Enable RRPP.
[DeviceC] rrpp enable

```


Configuring Device D

Create VLANs 2 through 30.

```
<DeviceD> system-view
[DeviceD] vlan 2 to 30
Please wait... Done.
```

Map these VLANs to MSTI 1.

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 2 to 30
```

Activate the MST region configuration.

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

Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

Set the trusted packet priority type to 802.1p priority on the port.

```
[DeviceD-GigabitEthernet1/0/1] qos trust dot1p
```

Configure the port as a trunk port.

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 2 through 30.

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceD-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] qos trust dot1p
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceD-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceD] rrpp domain 1
Info: Create a new domain.
```

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```
[DeviceD-rrpp-domain1] control-vlan 4092
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device D as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
```

```
[DeviceD-rrpp-domain1] quit
```

```
# Enable RRPP.
```

```
[DeviceD] rrpp enable
```

Configuring Device E

```
# Create VLANs 2 through 30.
```

```
<DeviceE> system-view
```

```
[DeviceE] vlan 2 to 30
```

```
Please wait... Done.
```

```
# Map these VLANs to MSTI 1.
```

```
[DeviceE] stp region-configuration
```

```
[DeviceE-mst-region] instance 1 vlan 2 to 30
```

```
# Activate the MST region configuration.
```

```
[DeviceE-mst-region] active region-configuration
```

```
[DeviceE-mst-region] quit
```

```
# Disable the spanning tree feature on GigabitEthernet 1/0/1.
```

```
[DeviceE] interface gigabitethernet 1/0/1
```

```
[DeviceE-GigabitEthernet1/0/1] undo stp enable
```

```
# Set the trusted packet priority type to 802.1p priority on the port.
```

```
[DeviceE-GigabitEthernet1/0/1] qos trust dot1p
```

```
# Configure the port as a trunk port.
```

```
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
```

```
# Assign the port to VLANs 2 through 30.
```

```
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
```

```
Please wait... Done.
```

```
[DeviceE-GigabitEthernet1/0/1] quit
```

```
# Configure GigabitEthernet 1/0/2.
```

```
[DeviceE] interface gigabitethernet 1/0/2
```

```
[DeviceE-GigabitEthernet1/0/2] undo stp enable
```

```
[DeviceE-GigabitEthernet1/0/2] qos trust dot1p
```

```
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
```

```
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
```

```
Please wait... Done.
```

```
[DeviceE-GigabitEthernet1/0/2] quit
```

```
# Create RRPP domain 1.
```

```
[DeviceE] rrpp domain 1
```

```
Info: Create a new domain.
```

```
# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
```

```
[DeviceE-rrpp-domain1] control-vlan 4092
```

```
# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
```

```
[DeviceE-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device E as the master node of subring 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 2.

```
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceE-rrpp-domain1] ring 2 enable
[DeviceE-rrpp-domain1] quit
```

Enable RRPP.

```
[DeviceE] rrpp enable
```

Verifying the configuration

Use the **display rrpp verbose** command to view RRPP configuration and operational information on each device. For more information, see "[Example: Configuring single ring.](#)"

Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
```

- ```

#
rrpp enable
#

```
- **Device B:**

```

#
vlan 2 to 30
#
stp region-configuration
instance 1 vlan 2 to 30
active region-configuration
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
rrpp domain 1
control-vlan 4092
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
ring 1 enable
ring 2 node-mode edge edge-port GigabitEthernet1/0/3
ring 2 enable
#
rrpp enable
#

```
  - **Device C:**

```

#
vlan 2 to 30
#
stp region-configuration

```

```

instance 1 vlan 2 to 30
active region-configuration
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
rrpp domain 1
control-vlan 4092
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
ring 1 enable
ring 2 node-mode assistant-edge edge-port GigabitEthernet1/0/3
ring 2 enable
#
rrpp enable
#

```

- **Device D:**

```

#
vlan 2 to 30
#
stp region-configuration
instance 1 vlan 2 to 30
active region-configuration
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable

```

```

qos trust dot1p
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
rrpp domain 1
control-vlan 4092
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
ring 1 enable
#
rrpp enable
#

```

- Device E:

```

#
vlan 2 to 30
#
stp region-configuration
instance 1 vlan 2 to 30
active region-configuration
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
rrpp domain 1
control-vlan 4092
protected-vlan reference-instance 1
ring 2 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
ring 2 enable
#
rrpp enable

```

#

# Example: Configuring dual homed rings

## Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

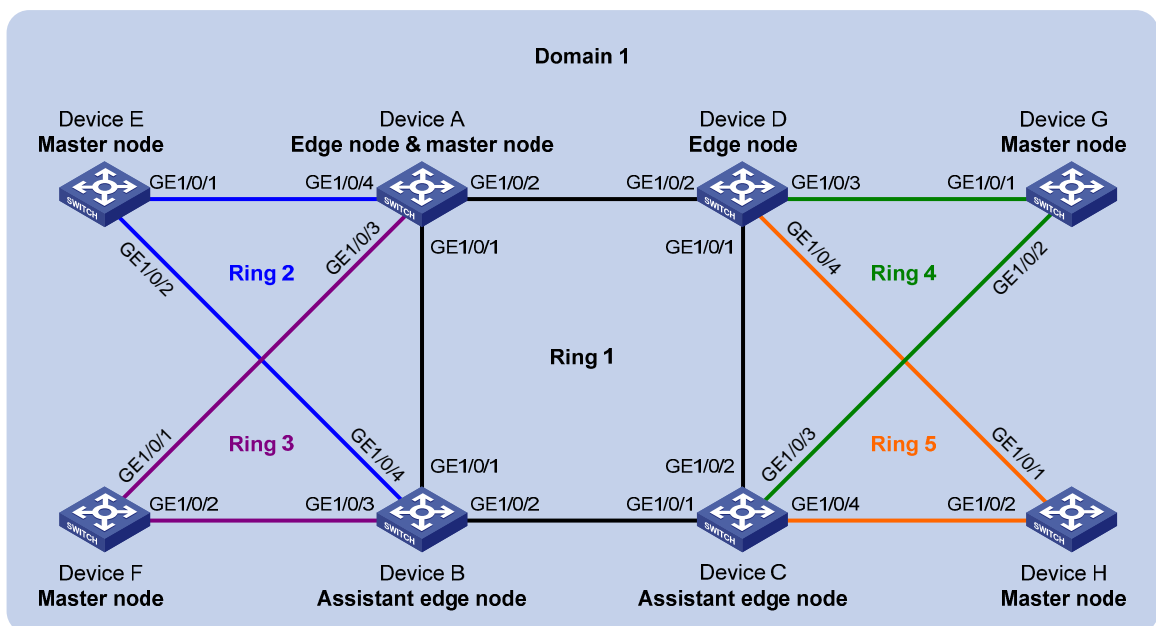
## Network requirements

As shown in [Figure 188](#), multiple access-layer devices are connected to the distribution layer by using a ring topology. The distribution layer also adopts a ring topology.

Configure RRPP to meet the following requirements:

- When all physical links on an Ethernet ring are connected:
  - The nodes on the ring can communicate with each another.
  - No broadcast storms can occur due to data loops.
- When a physical link on an Ethernet ring is broken, RRPP immediately restores communication between the nodes to ensure convergence performance of the network.
- When the broken link is restored, the link can forward data traffic again, and no loops occur.

**Figure 188 Network diagram**



## Requirements analysis

If multiple intersecting rings exist in an RRPP domain, configure the ring that connects all of them as the primary ring. In this example:

- Configure Ring 1 as the primary ring.
- Configure Ring 2 through Ring 5 as subrings.

For the primary ring, configure a device with high performance as the master node. For the subring, configure a device other than a common node as the master node. In this example:

- Configure Device A as the master node of Ring 1.
- Configure Device E, Device F, Device G, and Device H as the master node of Ring 2, Ring 3, Ring 4, and Ring 5, respectively.

## Configuration restrictions and guidelines

When you configure dual homed rings, follow these restrictions and guidelines:

- To avoid loops caused by disabling STP, perform full-mesh connection in the ring network after you complete RRPP configurations on all devices of the ring network.
- To activate an RRPP domain on the current device, enable the RRPP protocol and RRPP rings for the RRPP domain on the current device.
- To prevent Hello packets of subrings from being looped on the primary ring, enable the primary ring on its master node before you enable the subrings on their separate master nodes. On an edge node or assistant-edge node, enable the primary ring of an RRPP domain before you enable the subrings of the RRPP domain.
- For the HP 5500 EI & HP 5500 SI Switch Series, execute the **qos trust dot1p** command in Ethernet interface view to configure the 802.1p priority of trusted packets on RRPP ports. RRPP packets then take higher precedence than data packets when passing through the RRPP ports.

## Configuration procedures

### Configuring Device A

```
Create VLANs 2 through 30.
<DeviceA> system-view
[DeviceA] vlan 2 to 30
Please wait... Done.

Map these VLANs to MSTI 1.
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 2 to 30

Activate the MST region configuration.
```



```

[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit

Disable the spanning tree feature on GigabitEthernet 1/0/1.
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo stp enable

Set the trusted packet priority type to 802.1p priority on the port.
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p

Configure the port as a trunk port.
[DeviceA-GigabitEthernet1/0/1] port link-type trunk

Assign the port to VLANs 2 through 30.
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceA-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2.
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] quit

Configure GigabitEthernet 1/0/3.
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] undo stp enable
[DeviceA-GigabitEthernet1/0/3] qos trust dot1p
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceA-GigabitEthernet1/0/3] quit

Configure GigabitEthernet 1/0/4.
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] undo stp enable
[DeviceA-GigabitEthernet1/0/4] qos trust dot1p
[DeviceA-GigabitEthernet1/0/4] port link-type trunk
[DeviceA-GigabitEthernet1/0/4] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceA-GigabitEthernet1/0/4] quit

Create RRPP domain 1.
[DeviceA] rrpp domain 1
Info: Create a new domain.

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceA-rrpp-domain1] control-vlan 4092

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```

```

[DeviceA-rrpp-domain1] protected-vlan reference-instance 1

Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary
port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable

Configure Device A as the edge node of subring 2, with GigabitEthernet 1/0/4 as the edge port.
Enable subring 2.
[DeviceA-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceA-rrpp-domain1] ring 2 enable

Configure Device A as the edge node of subring 3, with GigabitEthernet 1/0/3 as the edge port.
Enable subring 3.
[DeviceA-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceA-rrpp-domain1] ring 3 enable
[DeviceA-rrpp-domain1] quit

Enable RRPP.
[DeviceA] rrpp enable

```

## Configuring Device B

```

Create VLANs 2 through 30.
<DeviceB> system-view
[DeviceB] vlan 2 to 30
Please wait... Done.

Map these VLANs to MSTI 1.
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 2 to 30

Activate the MST region configuration.
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit

Disable the spanning tree feature on GigabitEthernet 1/0/1.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo stp enable

Set the trusted packet priority type to 802.1p priority on the port.
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p

Configure the port as a trunk port.
[DeviceB-GigabitEthernet1/0/1] port link-type trunk

Assign the port to VLANs 2 through 30.
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceB-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2.
[DeviceB] interface gigabitethernet 1/0/2

```

```

[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceB-GigabitEthernet1/0/2] quit

Configure GigabitEthernet 1/0/3.
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] qos trust dot1p
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceB-GigabitEthernet1/0/3] quit

Configure GigabitEthernet 1/0/4.
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] undo stp enable
[DeviceB-GigabitEthernet1/0/4] qos trust dot1p
[DeviceB-GigabitEthernet1/0/4] port link-type trunk
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceB-GigabitEthernet1/0/4] quit

Create RRPP domain 1.
[DeviceB] rrpp domain 1
Info: Create a new domain.

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceB-rrpp-domain1] control-vlan 4092

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1

Configure Device B as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary
port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable

Configure Device B as the assistant-edge node of subring 2, with GigabitEthernet 1/0/4 as the edge
port. Enable subring 2.
[DeviceB-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/4
[DeviceB-rrpp-domain1] ring 2 enable

Configure Device B as the assistant-edge node of subring 3, with GigabitEthernet 1/0/3 as the edge
port. Enable subring 3.
[DeviceB-rrpp-domain1] ring 3 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceB-rrpp-domain1] ring 3 enable
[DeviceB-rrpp-domain1] quit

```

```
Enable RRPP.
[DeviceB] rrpp enable
```

## Configuring Device C

```
Create VLANs 2 through 30.
```

```
<DeviceC> system-view
[DeviceC] vlan 2 to 30
Please wait... Done.
```

```
Map these VLANs to MSTI 1.
```

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 2 to 30
```

```
Activate the MST region configuration.
```

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

```
Disable the spanning tree feature on GigabitEthernet 1/0/1.
```

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

```
Set the trusted packet priority type to 802.1p priority on the port.
```

```
[DeviceC-GigabitEthernet1/0/1] qos trust dot1p
```

```
Configure the port as a trunk port.
```

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

```
Assign the port to VLANs 2 through 30.
```

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceC-GigabitEthernet1/0/1] quit
```

```
Configure GigabitEthernet 1/0/2.
```

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] qos trust dot1p
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceC-GigabitEthernet1/0/2] quit
```

```
Configure GigabitEthernet 1/0/3.
```

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] qos trust dot1p
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceC-GigabitEthernet1/0/3] quit
```

```
Configure GigabitEthernet 1/0/4.
```

```
[DeviceC] interface gigabitethernet 1/0/4
```

```

[DeviceC-GigabitEthernet1/0/4] undo stp enable
[DeviceC-GigabitEthernet1/0/4] qos trust dot1p
[DeviceC-GigabitEthernet1/0/4] port link-type trunk
[DeviceC-GigabitEthernet1/0/4] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceC-GigabitEthernet1/0/4] quit

Create RRPP domain 1.
[DeviceC] rrpp domain 1
Info: Create a new domain.

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceC-rrpp-domain1] control-vlan 4092

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1

Configure Device C as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary
port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable

Configure Device C as the assistant-edge node of subring 4, with GigabitEthernet 1/0/3 as the edge
port. Enable subring 4.
[DeviceC-rrpp-domain1] ring 4 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain1] ring 4 enable

Configure Device C as the assistant-edge node of subring 5, with GigabitEthernet 1/0/4 as the edge
port. Enable subring 5.
[DeviceC-rrpp-domain1] ring 5 node-mode assistant-edge edge-port gigabitethernet 1/0/4
[DeviceC-rrpp-domain1] ring 5 enable
[DeviceC-rrpp-domain1] quit

Enable RRPP.
[DeviceC] rrpp enable

```

## Configuring Device D

```

Create VLANs 2 through 30.
<DeviceD> system-view
[DeviceD] vlan 2 to 30
Please wait... Done.

Map these VLANs to MSTI 1.
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 2 to 30

Activate the MST region configuration.
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit

Disable the spanning tree feature on GigabitEthernet 1/0/1.
[DeviceD] interface gigabitethernet 1/0/1

```

```

[DeviceD-GigabitEthernet1/0/1] undo stp enable

Set the trusted packet priority type to 802.1p priority on the port.
[DeviceD-GigabitEthernet1/0/1] qos trust dot1p

Configure the port as a trunk port.
[DeviceD-GigabitEthernet1/0/1] port link-type trunk

Assign the port to VLANs 2 through 30.
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceD-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2.
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] qos trust dot1p
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceD-GigabitEthernet1/0/2] quit

Configure GigabitEthernet 1/0/3.
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] undo stp enable
[DeviceD-GigabitEthernet1/0/3] qos trust dot1p
[DeviceD-GigabitEthernet1/0/3] port link-type trunk
[DeviceD-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceD-GigabitEthernet1/0/3] quit

Configure GigabitEthernet 1/0/4.
[DeviceD] interface gigabitethernet 1/0/4
[DeviceD-GigabitEthernet1/0/4] undo stp enable
[DeviceD-GigabitEthernet1/0/4] qos trust dot1p
[DeviceD-GigabitEthernet1/0/4] port link-type trunk
[DeviceD-GigabitEthernet1/0/4] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceD-GigabitEthernet1/0/4] quit

Create RRPP domain 1.
[DeviceD] rrpp domain 1
Info: Create a new domain.

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceD-rrpp-domain1] control-vlan 4092

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1

Configure Device D as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary
port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
```

# Configure Device D as the edge node of subring 4, with GigabitEthernet 1/0/3 as the edge port.  
Enable subring 4.

```
[DeviceD-rrpp-domain1] ring 4 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceD-rrpp-domain1] ring 4 enable
```

# Configure Device D as the edge node of subring 5, with GigabitEthernet 1/0/4 as the edge port.  
Enable subring 5.

```
[DeviceD-rrpp-domain1] ring 5 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceD-rrpp-domain1] ring 5 enable
[DeviceD-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceD] rrpp enable
```

## Configuring Device E

# Create VLANs 2 through 30.

```
<DeviceE> system-view
[DeviceE] vlan 2 to 30
Please wait... Done.
```

# Map these VLANs to MSTI 1.

```
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 1 vlan 2 to 30
```

# Activate the MST region configuration.

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

# Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo stp enable
```

# Set the trusted packet priority type to 802.1p priority on the port.

```
[DeviceE-GigabitEthernet1/0/1] qos trust dot1p
```

# Configure the port as a trunk port.

```
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
```

# Assign the port to VLANs 2 through 30.

```
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceE-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2.

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] qos trust dot1p
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
```

```

Please wait... Done.
[DeviceE-GigabitEthernet1/0/2] quit

Create RRPP domain 1.
[DeviceE] rrpp domain 1
Info: Create a new domain.

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceE-rrpp-domain1] control-vlan 4092

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceE-rrpp-domain1] protected-vlan reference-instance 1

Configure Device E as the master node of subring 2, with GigabitEthernet 1/0/1 as the primary port
and GigabitEthernet 1/0/2 as the secondary port. Enable subring 2.
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceE-rrpp-domain1] ring 2 enable
[DeviceE-rrpp-domain1] quit

Enable RRPP.
[DeviceE] rrpp enable

```

## Configuring Device F

```

Create VLANs 2 through 30.
<DeviceF> system-view
[DeviceF] vlan 2 to 30
Please wait... Done.

Map these VLANs to MSTI 1.
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 2 to 30

Activate the MST region configuration.
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit

Disable the spanning tree feature on GigabitEthernet 1/0/1.
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] undo stp enable

Set the trusted packet priority type to 802.1p priority on the port.
[DeviceF-GigabitEthernet1/0/1] qos trust dot1p

Configure the port as a trunk port.
[DeviceF-GigabitEthernet1/0/1] port link-type trunk

Assign the port to VLANs 2 through 30.
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceF-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2.
[DeviceF] interface gigabitethernet 1/0/2

```



```

[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] qos trust dot1p
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceF-GigabitEthernet1/0/2] quit

Create RRPP domain 1.
[DeviceF] rrpp domain 1
Info: Create a new domain.

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceF-rrpp-domain1] control-vlan 4092

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceF-rrpp-domain1] protected-vlan reference-instance 1

Configure Device F as the master node of subring 3, with GigabitEthernet 1/0/1 as the primary port
and GigabitEthernet 1/0/2 as the secondary port. Enable subring 3.
[DeviceF-rrpp-domain1] ring 3 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceF-rrpp-domain1] ring 3 enable
[DeviceF-rrpp-domain1] quit

Enable RRPP.
[DeviceF] rrpp enable

```

## Configuring Device G

```

Create VLANs 2 through 30.
<DeviceG> system-view
[DeviceG] vlan 2 to 30
Please wait... Done.

Map these VLANs to MSTI 1.
[DeviceG] stp region-configuration
[DeviceG-mst-region] instance 1 vlan 2 to 30

Activate the MST region configuration.
[DeviceG-mst-region] active region-configuration
[DeviceG-mst-region] quit

Disable the spanning tree feature on GigabitEthernet 1/0/1.
[DeviceG] interface gigabitethernet 1/0/1
[DeviceG-GigabitEthernet1/0/1] undo stp enable

Set the trusted packet priority type to 802.1p priority on the port.
[DeviceG-GigabitEthernet1/0/1] qos trust dot1p

Configure the port as a trunk port.
[DeviceG-GigabitEthernet1/0/1] port link-type trunk

Assign the port to VLANs 2 through 30.
[DeviceG-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30

```

```

Please wait... Done.
[DeviceG-GigabitEthernet1/0/1] quit
Configure GigabitEthernet 1/0/2.
[DeviceG] interface gigabitethernet 1/0/2
[DeviceG-GigabitEthernet1/0/2] undo stp enable
[DeviceG-GigabitEthernet1/0/2] qos trust dot1p
[DeviceG-GigabitEthernet1/0/2] port link-type trunk
[DeviceG-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceG-GigabitEthernet1/0/2] quit
Create RRPP domain 1.
[DeviceG] rrpp domain 1
Info: Create a new domain.
Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceG-rrpp-domain1] control-vlan 4092
Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceG-rrpp-domain1] protected-vlan reference-instance 1
Configure Device G as the master node of subring 4, with GigabitEthernet 1/0/1 as the primary port
and GigabitEthernet 1/0/2 as the secondary port. Enable subring 4.
[DeviceG-rrpp-domain1] ring 4 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceG-rrpp-domain1] ring 4 enable
[DeviceG-rrpp-domain1] quit
Enable RRPP.
[DeviceG] rrpp enable

```

## Configuring Device H

```

Create VLANs 2 through 30.
<DeviceH> system-view
[DeviceH] vlan 2 to 30
Please wait... Done.
Map these VLANs to MSTI 1.
[DeviceH] stp region-configuration
[DeviceH-mst-region] instance 1 vlan 2 to 30
Activate the MST region configuration.
[DeviceH-mst-region] active region-configuration
[DeviceH-mst-region] quit
Disable the spanning tree feature on GigabitEthernet 1/0/1.
[DeviceH] interface gigabitethernet 1/0/1
[DeviceH-GigabitEthernet1/0/1] undo stp enable
Set the trusted packet priority type to 802.1p priority on the port.
[DeviceH-GigabitEthernet1/0/1] qos trust dot1p
Configure the port as a trunk port.

```

```

[DeviceH-GigabitEthernet1/0/1] port link-type trunk

Assign the port to VLANs 2 through 30.
[DeviceH-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceH-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2.
[DeviceH] interface gigabitethernet 1/0/2
[DeviceH-GigabitEthernet1/0/2] undo stp enable
[DeviceH-GigabitEthernet1/0/2] qos trust dot1p
[DeviceH-GigabitEthernet1/0/2] port link-type trunk
[DeviceH-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceH-GigabitEthernet1/0/2] quit

Create RRPP domain 1.
[DeviceH] rrpp domain 1
Info: Create a new domain.

Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceH-rrpp-domain1] control-vlan 4092

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceH-rrpp-domain1] protected-vlan reference-instance 1

Configure Device H as the master node of subring 5, with GigabitEthernet 1/0/1 as the primary port
and GigabitEthernet 1/0/2 as the secondary port. Enable subring 5.
[DeviceH-rrpp-domain1] ring 5 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceH-rrpp-domain1] ring 5 enable
[DeviceH-rrpp-domain1] quit

Enable RRPP.
[DeviceH] rrpp enable

```

## Verifying the configuration

# Use the **display rrpp verbose** command to view RRPP configuration and operational information on each device. For more information, see "[Example: Configuring single ring.](#)"

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```

#
vlan 2 to 30
#
stp region-configuration

```

```

instance 1 vlan 2 to 30
active region-configuration
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/4
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
rrpp domain 1
control-vlan 4092
protected-vlan reference-instance 1
ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
ring 1 enable
ring 2 node-mode edge edge-port GigabitEthernet1/0/4
ring 2 enable
ring 3 node-mode edge edge-port GigabitEthernet1/0/3
ring 3 enable
#
rrpp enable
#
• Device B:
#
vlan 2 to 30
#

```

```

stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge edge-port GigabitEthernet1/0/4
 ring 2 enable
 ring 3 node-mode assistant-edge edge-port GigabitEthernet1/0/3
 ring 3 enable
#
rrpp enable
#
• Device C:
#
vlan 2 to 30

```

```

#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 4 node-mode assistant-edge edge-port GigabitEthernet1/0/3
 ring 4 enable
 ring 5 node-mode assistant-edge edge-port GigabitEthernet1/0/4
 ring 5 enable
#
rrpp enable
#

```

- Device D:

```

#

```

```

vlan 2 to 30
#
stp region-configuration
instance 1 vlan 2 to 30
active region-configuration
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/4
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
rrpp domain 1
control-vlan 4092
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
ring 1 enable
ring 4 node-mode edge edge-port GigabitEthernet1/0/3
ring 4 enable
ring 5 node-mode edge edge-port GigabitEthernet1/0/4
ring 5 enable
#
rrpp enable
#

```

- Device E:

```

#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 2 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
 GigabitEthernet1/0/2 level 1
 ring 2 enable
#
rrpp enable
#

```

- **Device F:**

```

#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk

```



```

port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
rrpp domain 1
control-vlan 4092
protected-vlan reference-instance 1
ring 3 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
ring 3 enable
#
rrpp enable
#

```

- **Device G:**

```

#
vlan 2 to 30
#
stp region-configuration
instance 1 vlan 2 to 30
active region-configuration
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 2 to 30
stp disable
qos trust dot1p
#
rrpp domain 1
control-vlan 4092
protected-vlan reference-instance 1
ring 4 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
ring 4 enable
#
rrpp enable
#

```

- **Device H:**

```

#
vlan 2 to 30
#

```

```

stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 qos trust dot1p
#
rrpp domain 1
 control-vlan 4092
 protected-vlan reference-instance 1
 ring 5 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
 ring 5 enable
#
rrpp enable
#

```

## Example: Configuring load balanced intersecting-ring

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

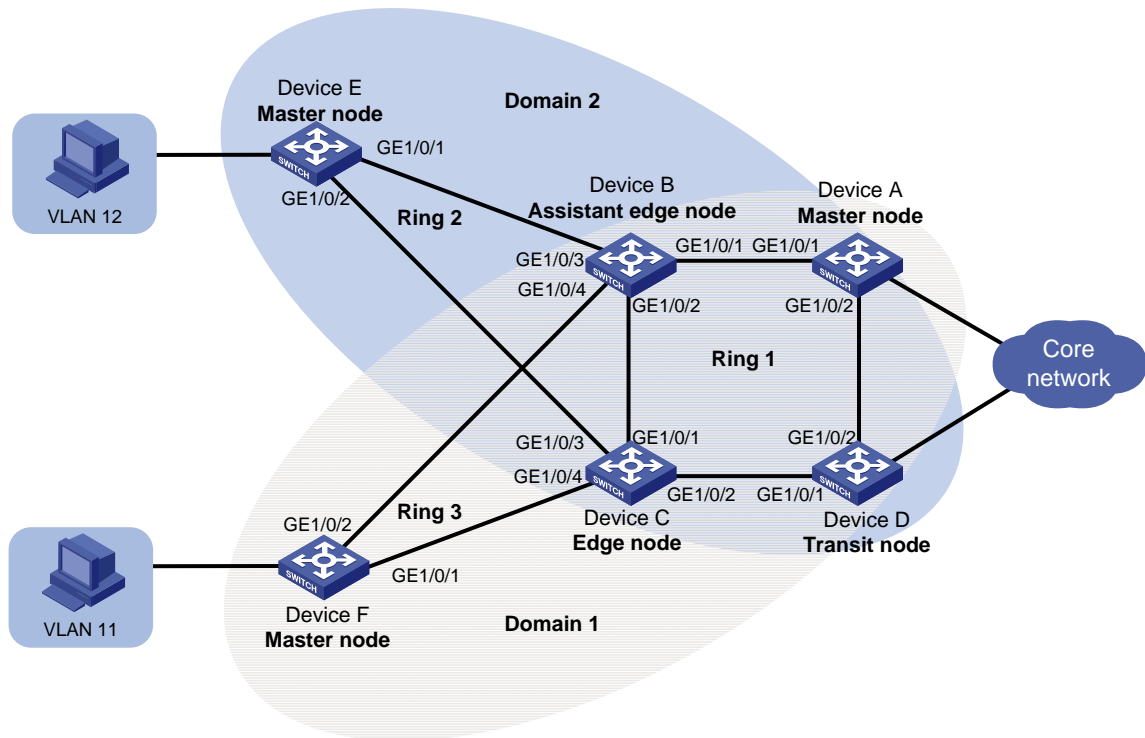
### Network requirements

As shown in [Figure 189](#), two access-layer networks are connected to the distribution layer by using a ring topology. The distribution layer also adopts a ring topology.

Configure RRPP to meet the following requirements:

- High availability and convergence performance of the network.
- Traffic load sharing by VLAN. (Traffic of VLAN 12 is forwarded through domain 2, and traffic of VLAN 11 is forwarded through domain 1.)
- Reduced number of Edge-Hello packets.

**Figure 189 Network diagram**



## Requirements analysis

To forward traffic of different VLANs through different domains (paths), configure multiple domains for a ring network. In this example:

- Configure Ring 1 and Ring 3 as the primary ring and subring for domain 1.
- Configure Ring 1 and Ring 2 as the primary ring and subring for domain 2.

The primary ring must feature high transmission capability for transparently transmitting traffic of the protected VLANs and control VLANs of the subrings. In this example:

- Configure Ring 1 as the primary ring of both domain 1 and domain 2.
- Configure Ring 2 and Ring 3 as the subrings of domain 2 and domain 1, respectively.

For the primary ring, configure a device with high performance as the master node. For the subring, configure a device other than a common node as the master node. In this example:

- Configure Device A as the master node of Ring 1.
- Configure Device E and Device F as the master node of Ring 2 and Ring 3, respectively.

To reduce Edge-Hello traffic, adopt the RRPP ring group mechanism by assigning Ring 2 and Ring 3 with the same edge node and assistant-edge node to a RRPP ring group.

## Configuration restrictions and guidelines

When you configure load balanced intersecting-ring, follow these restrictions and guidelines:

- To avoid loops caused by disabling STP, perform full-mesh connection in the ring network after you complete RRPP configurations on all devices of the ring network.
- To activate an RRPP domain on the current device, enable the RRPP protocol and RRPP rings for the RRPP domain on the current device.
- To prevent Hello packets of subrings from being looped on the primary ring, enable the primary ring on its master node before you enable the subrings on their separate master nodes. On an edge node or assistant-edge node, enable the primary ring of an RRPP domain before you enable the subrings of the RRPP domain.
- To assign an active ring to a ring group, do that on the assistant-edge node first and then on the edge node.
- Make sure the RRPP ring group on the edge node and the RRPP ring group on the assistant-edge node have the same configurations and activation status.
- For the HP 5500 EI & HP 5500 SI Switch Series, execute the **qos trust dot1p** command in Ethernet interface view to configure the 802.1p priority of trusted packets on RRPP ports. RRPP packets then take higher precedence than data packets when passing through the RRPP ports.

## Configuration procedures

### Configuring Device A

```
Create VLANs 11 and 12.
<DeviceA> system-view
[DeviceA] vlan 11 to 12
Please wait... Done.

Map VLAN 11 to MSTI 1 and VLAN 12 to MSTI 2.
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 11
[DeviceA-mst-region] instance 2 vlan 12

Activate the MST region configuration.
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit

Disable the spanning tree feature on GigabitEthernet 1/0/1.
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo stp enable

Set the trusted packet priority type to 802.1p priority on the port.
```

```

[DeviceA-GigabitEthernet1/0/1] qos trust dot1p

Configure the port as a trunk port.
[DeviceA-GigabitEthernet1/0/1] port link-type trunk

Remove the port from VLAN 1.
[DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
Please wait... Done.

Assign the port to VLAN 11 and VLAN 12.
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 11 12
Please wait... Done.

Configure VLAN 11 as the default VLAN.
[DeviceA-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceA-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2.
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 11 12
Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceA-GigabitEthernet1/0/2] quit

Create RRPP domain 1.
[DeviceA] rrpp domain 1
Info: Create a new domain.

Configure VLAN 100 as the primary control VLAN of RRPP domain 1.
[DeviceA-rrpp-domain1] control-vlan 100

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1

Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary
port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit

Create RRPP domain 2.
[DeviceA] rrpp domain 2
Info: Create a new domain.

Configure VLAN 105 as the primary control VLAN of RRPP domain 2.
[DeviceA-rrpp-domain2] control-vlan 105

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```

```
[DeviceA-rrpp-domain2] protected-vlan reference-instance 2

Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/2 as the primary
port and GigabitEthernet 1/0/1 as the secondary port. Enable ring 1.

[DeviceA-rrpp-domain2] ring 1 node-mode master primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 0
[DeviceA-rrpp-domain2] ring 1 enable
[DeviceA-rrpp-domain2] quit

Enable RRPP.
[DeviceA] rrpp enable
```

## Configuring Device B

```
Create VLANs 11 and 12.
<DeviceB> system-view
[DeviceB] vlan 11 to 12
Please wait... Done.

Map VLAN 11 to MSTI 1 and VLAN 12 to MSTI 2.
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 11
[DeviceB-mst-region] instance 2 vlan 12

Activate the MST region configuration.
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit

Disable the spanning tree feature on GigabitEthernet 1/0/1.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo stp enable

Set the trusted packet priority type to 802.1p priority on the port.
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p

Configure the port as a trunk port.
[DeviceB-GigabitEthernet1/0/1] port link-type trunk

Remove the port from VLAN 1.
[DeviceB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
Please wait... Done.

Assign the port to VLAN 11 and VLAN 12.
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 11 12
Please wait... Done.

Configure VLAN 11 as the default VLAN.
[DeviceB-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceB-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2.
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
```

```

[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] undo port trunk permit vlan 1
Please wait... Done.
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 11 12
Please wait... Done.
[DeviceB-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceB-GigabitEthernet1/0/2] quit

Disable the spanning tree feature on GigabitEthernet 1/0/3.
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] undo stp enable

Set the trusted packet priority type to 802.1p priority on the port.
[DeviceB-GigabitEthernet1/0/3] qos trust dot1p

Configure the port as a trunk port.
[DeviceB-GigabitEthernet1/0/3] port link-type trunk

Remove the port from VLAN 1.
[DeviceB-GigabitEthernet1/0/3] undo port trunk permit vlan 1
Please wait... Done.

Assign the port to VLAN 12.
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 12
Please wait... Done.

Configure VLAN 12 as the default VLAN.
[DeviceB-GigabitEthernet1/0/3] port trunk pvid vlan 12
[DeviceB-GigabitEthernet1/0/3] quit

Disable the spanning tree feature on GigabitEthernet 1/0/4.
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] undo stp enable

Set the trusted packet priority type to 802.1p priority on the port.
[DeviceB-GigabitEthernet1/0/4] qos trust dot1p

Configure the port as a trunk port.
[DeviceB-GigabitEthernet1/0/4] port link-type trunk

Remove the port from VLAN 1.
[DeviceB-GigabitEthernet1/0/4] undo port trunk permit vlan 1
Please wait... Done.

Assign the port to VLAN 11.
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 11
Please wait... Done.

Configure VLAN 11 as the default VLAN.
[DeviceB-GigabitEthernet1/0/4] port trunk pvid vlan 11
[DeviceB-GigabitEthernet1/0/4] quit

Create RRPP domain 1.
[DeviceB] rrpp domain 1

```

Info: Create a new domain.

# Configure VLAN 100 as the primary control VLAN of RRPP domain 1.

```
[DeviceB-rrpp-domain1] control-vlan 100
```

# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device B as a transit node of primary ring 1 in RRPP domain 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

```
[DeviceB-rrpp-domain1] ring 1 enable
```

# Configure Device B as the assistant-edge node of subring 3 in RRPP domain 1, with GigabitEthernet 1/0/4 as the edge port. Enable subring 3.

```
[DeviceB-rrpp-domain1] ring 3 node-mode assistant-edge edge-port gigabitethernet 1/0/4
```

```
[DeviceB-rrpp-domain1] ring 3 enable
```

```
[DeviceB-rrpp-domain1] quit
```

# Create RRPP domain 2.

```
[DeviceB] rrpp domain 2
```

Info: Create a new domain.

# Configure VLAN 105 as the primary control VLAN of RRPP domain 2.

```
[DeviceB-rrpp-domain2] control-vlan 105
```

# Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceB-rrpp-domain2] protected-vlan reference-instance 2
```

# Configure Device B as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceB-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

```
[DeviceB-rrpp-domain2] ring 1 enable
```

# Configure Device B as the assistant-edge node of subring 2 in RRPP domain 2, with GigabitEthernet 1/0/3 as the edge port. Enable subring 2.

```
[DeviceB-rrpp-domain2] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
```

```
[DeviceB-rrpp-domain2] ring 2 enable
```

```
[DeviceB-rrpp-domain2] quit
```

# Enable RRPP.

```
[DeviceB] rrpp enable
```

## Configuring Device C

# Create VLANs 11 and 12.

```
<DeviceC> system-view
```

```
[DeviceC] vlan 11 to 12
```

```
Please wait... Done.
```

# Map VLAN 11 to MSTI 1 and VLAN 12 to MSTI 2.

```
[DeviceC] stp region-configuration
```



```

[DeviceC-mst-region] instance 1 vlan 11
[DeviceC-mst-region] instance 2 vlan 12

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

Disable the spanning tree feature on GigabitEthernet 1/0/1.
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo stp enable

Set the trusted packet priority type to 802.1p priority on the port.
[DeviceC-GigabitEthernet1/0/1] qos trust dot1p

Configure the port as a trunk port.
[DeviceC-GigabitEthernet1/0/1] port link-type trunk

Remove the port from VLAN 1.
[DeviceC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
Please wait... Done.

Assign the port to VLAN 11 and VLAN 12.
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 11 12
Please wait... Done.

Configure VLAN 11 as the default VLAN.
[DeviceC-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceC-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2.
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] qos trust dot1p
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
Please wait... Done.
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 11 12
Please wait... Done.
[DeviceC-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceC-GigabitEthernet1/0/2] quit

Disable the spanning tree feature on GigabitEthernet 1/0/3.
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo stp enable

Set the trusted packet priority type to 802.1p priority on the port.
[DeviceC-GigabitEthernet1/0/3] qos trust dot1p

Configure the port as a trunk port.
[DeviceC-GigabitEthernet1/0/3] port link-type trunk

Remove the port from VLAN 1.
[DeviceC-GigabitEthernet1/0/3] undo port trunk permit vlan 1
Please wait... Done.

```

```

Assign the port to VLAN 12.
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 12
Please wait... Done.

Configure VLAN 12 as the default VLAN.
[DeviceC-GigabitEthernet1/0/3] port trunk pvid vlan 12
[DeviceC-GigabitEthernet1/0/3] quit

Disable the spanning tree feature on GigabitEthernet 1/0/4.
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] undo stp enable

Set the trusted packet priority type to 802.1p priority on the port.
[DeviceC-GigabitEthernet1/0/4] qos trust dot1p

Configure the port as a trunk port.
[DeviceC-GigabitEthernet1/0/4] port link-type trunk

Remove the port from VLAN 1.
[DeviceC-GigabitEthernet1/0/4] undo port trunk permit vlan 1
Please wait... Done.

Assign the port to VLAN 11.
[DeviceC-GigabitEthernet1/0/4] port trunk permit vlan 11
Please wait... Done.

Configure VLAN 11 as the default VLAN.
[DeviceC-GigabitEthernet1/0/4] port trunk pvid vlan 11
[DeviceC-GigabitEthernet1/0/4] quit

Create RRPP domain 1.
[DeviceC] rrpp domain 1
Info: Create a new domain.

Configure VLAN 100 as the primary control VLAN of RRPP domain 1.
[DeviceC-rrpp-domain1] control-vlan 100

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1

Configure Device C as the transit node of primary ring 1 in RRPP domain 1, with GigabitEthernet
1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable

Configure Device C as the edge node of subring 3 in RRPP domain 1, with GigabitEthernet 1/0/4 as
the edge port. Enable subring 3.
[DeviceC-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceC-rrpp-domain1] ring 3 enable
[DeviceC-rrpp-domain1] quit

Create RRPP domain 2.
[DeviceC] rrpp domain 2

```

Info: Create a new domain.

# Configure VLAN 105 as the primary control VLAN of RRPP domain 2.

```
[DeviceC-rrpp-domain2] control-vlan 105
```

# Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceC-rrpp-domain2] protected-vlan reference-instance 2
```

# Configure Device C as the transit node of primary ring 1 in RRPP domain 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceC-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

```
[DeviceC-rrpp-domain2] ring 1 enable
```

# Configure Device C as the edge node of subring 2 in RRPP domain 2, with GigabitEthernet 1/0/3 as the edge port. Enable subring 2.

```
[DeviceC-rrpp-domain2] ring 2 node-mode edge edge-port gigabitethernet1/0/3
```

```
[DeviceC-rrpp-domain2] ring 2 enable
```

```
[DeviceC-rrpp-domain2] quit
```

# Enable RRPP.

```
[DeviceC] rrpp enable
```

## Configuring Device D

# Create VLANs 11 and 12.

```
<DeviceD> system-view
```

```
[DeviceD] vlan 11 to 12
```

```
Please wait... Done.
```

# Map VLAN 11 to MSTI 1 and VLAN 12 to MSTI 2.

```
[DeviceD] stp region-configuration
```

```
[DeviceD-mst-region] instance 1 vlan 11
```

```
[DeviceD-mst-region] instance 2 vlan 12
```

# Activate the MST region configuration.

```
[DeviceD-mst-region] active region-configuration
```

```
[DeviceD-mst-region] quit
```

# Disable the spanning tree feature on GigabitEthernet 1/0/1.

```
[DeviceD] interface gigabitethernet 1/0/1
```

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

# Set the trusted packet priority type to 802.1p priority on the port.

```
[DeviceD-GigabitEthernet1/0/1] qos trust dot1p
```

# Configure the port as a trunk port.

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

# Remove the port from VLAN 1.

```
[DeviceD-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
Please wait... Done.
```

# Assign the port to VLAN 11 and VLAN 12.

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 11 12
```

Please wait... Done.

**# Configure VLAN 11 as the default VLAN.**

```
[DeviceD-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceD-GigabitEthernet1/0/1] quit
```

**# Configure GigabitEthernet 1/0/2.**

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] qos trust dot1p
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] undo port trunk permit vlan 1
Please wait... Done.
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 11 12
Please wait... Done.
[DeviceD-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceD-GigabitEthernet1/0/2] quit
```

**# Create RRPP domain 1.**

```
[DeviceD] rrpp domain 1
Info: Create a new domain.
```

**# Configure VLAN 100 as the primary control VLAN of RRPP domain 1.**

```
[DeviceD-rrpp-domain1] control-vlan 100
```

**# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.**

```
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

**# Configure Device D as the transit node of primary ring 1 in RRPP domain 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.**

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
[DeviceD-rrpp-domain1] quit
```

**# Create RRPP domain 2.**

```
[DeviceD] rrpp domain 2
Info: Create a new domain.
```

**# Configure VLAN 105 as the primary control VLAN of RRPP domain 2.**

```
[DeviceD-rrpp-domain2] control-vlan 105
```

**# Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.**

```
[DeviceD-rrpp-domain2] protected-vlan reference-instance 2
```

**# Configure Device D as the transit node of primary ring 1 in RRPP domain 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.**

```
[DeviceD-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain2] ring 1 enable
[DeviceD-rrpp-domain2] quit
```

**# Enable RRPP.**

```
[DeviceD] rrpp enable
```

## Configuring Device E

```
Create VLAN 12.
<DeviceE> system-view
[DeviceE] vlan 12
 Please wait... Done.
[DeviceE-vlan12] quit

Map VLAN 12 to MSTI 2
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 2 vlan 12

Activate the MST region configuration.
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit

Disable the spanning tree feature on GigabitEthernet 1/0/1.
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo stp enable

Set the trusted packet priority type to 802.1p priority on the port.
[DeviceE-GigabitEthernet1/0/1] qos trust dot1p

Configure the port as a trunk port.
[DeviceE-GigabitEthernet1/0/1] port link-type trunk

Remove the port from VLAN 1.
[DeviceE-GigabitEthernet1/0/1] undo port trunk permit vlan 1
 Please wait... Done.

Assign the port to VLAN 12.
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 12
 Please wait... Done.

Configure VLAN 12 as the default VLAN.
[DeviceE-GigabitEthernet1/0/1] port trunk pvid vlan 12
[DeviceE-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2.
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] qos trust dot1p
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] undo port trunk permit vlan 1
 Please wait... Done.
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 12
 Please wait... Done.
[DeviceE-GigabitEthernet1/0/2] port trunk pvid vlan 12
[DeviceE-GigabitEthernet1/0/2] quit

Create RRPP domain 2.
[DeviceE] rrpp domain 2
 Info: Create a new domain.
```

```

Configure VLAN 105 as the primary control VLAN of RRPP domain 2.
[DeviceE-rrpp-domain2] control-vlan 105

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.
[DeviceE-rrpp-domain2] protected-vlan reference-instance 2

Configure Device E as the master mode of subring 2 in RRPP domain 2, with GigabitEthernet 1/0/1
as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 2.
[DeviceE-rrpp-domain2] ring 2 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceE-rrpp-domain2] ring 2 enable
[DeviceE-rrpp-domain2] quit

Enable RRPP.
[DeviceE] rrpp enable

```

## Configuring Device F

```

Create VLAN 11.
<DeviceF> system-view
[DeviceF] vlan 11
 Please wait... Done.
[DeviceF-vlan11] quit

Map VLAN 11 to MSTI 1.
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 11

Activate the MST region configuration.
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit

Disable the spanning tree feature on GigabitEthernet 1/0/1.
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] undo stp enable

Set the trusted packet priority type to 802.1p priority on the port.
[DeviceF-GigabitEthernet1/0/1] qos trust dot1p

Configure the port as a trunk port.
[DeviceF-GigabitEthernet1/0/1] port link-type trunk

Remove the port from VLAN 1.
[DeviceF-GigabitEthernet1/0/1] undo port trunk permit vlan 1
 Please wait... Done.

Assign the port to VLAN 11.
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 11
 Please wait... Done.

Configure VLAN 11 as the default VLAN.
[DeviceF-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceF-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2.

```

```

[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] qos trust dot1p
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] undo port trunk permit vlan 1
Please wait... Done.
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 11
Please wait... Done.
[DeviceF-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceF-GigabitEthernet1/0/2] quit

Create RRPP domain 1.
[DeviceF] rrpp domain 1
Info: Create a new domain.

Configure VLAN 100 as the primary control VLAN of RRPP domain 1.
[DeviceF-rrpp-domain1] control-vlan 100

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceF-rrpp-domain1] protected-vlan reference-instance 1

Configure Device F as the master node of subring 3 in RRPP domain 1, with GigabitEthernet 1/0/1 as
the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable subring 3.
[DeviceF-rrpp-domain1] ring 3 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceF-rrpp-domain1] ring 3 enable
[DeviceF-rrpp-domain1] quit

Enable RRPP.
[DeviceF] rrpp enable

```

## Configuring RRPP ring groups on Device B and Device C

```

Create RRPP ring group 1 on Device B. Add subrings 2 and 3 to the RRPP ring group.
[DeviceB] rrpp ring-group 1
[DeviceB-rrpp-ring-group1] domain 2 ring 2
[DeviceB-rrpp-ring-group1] domain 1 ring 3

Create RRPP ring group 1 on Device C. Add subrings 2 and 3 to the RRPP ring group.
[DeviceC] rrpp ring-group 1
[DeviceC-rrpp-ring-group1] domain 2 ring 2
[DeviceC-rrpp-ring-group1] domain 1 ring 3

```

## Verifying the configuration

# Use the **display rrpp verbose** command to view RRPP configuration and operational information on each device. For more information, see "[Example: Configuring single ring.](#)"

# Display the brief RRPP information.

```

<DeviceA> display rrpp brief
Flags for Node Mode :

```

M -- Master , T -- Transit , E -- Edge , A -- Assistant-Edge

RRPP Protocol Status: Enable

Number of RRPP Domains: 2

```
Domain ID : 1
Control VLAN : Major 100 Sub 101
Protected VLAN: Reference Instance 1
Hello Timer : 1 sec Fail Timer : 3 sec
Ring Ring Node Primary/Common Secondary/Edge Enable
 ID Level Mode Port Port Status

 1 0 M GE1/0/1 GE1/0/2 Yes
```

```
Domain ID : 2
Control VLAN : Major 105 Sub 106
Protected VLAN: Reference Instance 2
Hello Timer : 1 sec Fail Timer : 3 sec
Ring Ring Node Primary/Common Secondary/Edge Enable
 ID Level Mode Port Port Status

 1 0 M GE1/0/1 GE1/0/2 Yes
```

The output shows that:

- The VLAN mapped to MSTI 1 is the protected VLAN of RRPP domain 1.
- The VLAN mapped to MSTI 2 is the protected VLAN of RRPP domain 2.

In this example, VLAN 11 is mapped to MSTI 1 and VLAN 12 is mapped to MSTI 2. Therefore, traffic from VLAN 11 and VLAN 12 is forwarded through RRPP domain 1 and RRPP domain 2, respectively.

# Display the RRPP ring group configuration.

```
<DeviceB> display rrpp ring-group
Ring Group 1:
Domain 1 Ring 3
Domain 2 Ring 2
Domain 1 Ring 3 is the sending ring
```

The output shows that RRPP group 1 takes effect, and only Ring 3 on Device B sends Edge-Hello packets.

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```
#
vlan 11 to 12
#
stp region-configuration
instance 1 vlan 11
```



```

instance 2 vlan 12
active region-configuration
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 11 to 12
port trunk pvid vlan 11
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 11 to 12
port trunk pvid vlan 11
stp disable
qos trust dot1p
#
rrpp domain 1
control-vlan 100
protected-vlan reference-instance 1
ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
ring 1 enable
#
rrpp domain 2
control-vlan 105
protected-vlan reference-instance 1
ring 1 node-mode master primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 0
ring 1 enable
#
rrpp enable
#

```

- **Device B:**

```

#
vlan 11 to 12
#
stp region-configuration
instance 1 vlan 11
instance 2 vlan 12
active region-configuration
#
interface GigabitEthernet1/0/1
port link-mode bridge

```

```

port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 11 to 12
port trunk pvid vlan 11
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 11 to 12
port trunk pvid vlan 11
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 12
port trunk pvid vlan 12
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/4
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 11
port trunk pvid vlan 11
stp disable
qos trust dot1p
#
rrpp domain 1
control-vlan 100
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
ring 1 enable
ring 3 node-mode assistant-edge edge-port GigabitEthernet1/0/4
ring 3 enable
#
rrpp domain 2
control-vlan 105
protected-vlan reference-instance 2
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
ring 1 enable

```

```

ring 2 node-mode assistant-edge edge-port GigabitEthernet1/0/3
ring 2 enable
#
rrpp ring-group 1
domain 2 ring 2
domain 1 ring 3
#
rrpp enable
#

```

- Device C:

```

#
vlan 11 to 12
#
stp region-configuration
instance 1 vlan 11
instance 2 vlan 12
active region-configuration
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 11 to 12
port trunk pvid vlan 11
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 11 to 12
port trunk pvid vlan 11
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 12
port trunk pvid vlan 12
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/4
port link-mode bridge
port link-type trunk

```

```

undo port trunk permit vlan 1
port trunk permit vlan 11
port trunk pvid vlan 11
stp disable
qos trust dot1p
#
rrpp domain 1
control-vlan 100
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
ring 1 enable
ring 3 node-mode edge edge-port GigabitEthernet1/0/4
ring 3 enable
#
rrpp domain 2
control-vlan 105
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
ring 1 enable
ring 2 node-mode edge edge-port GigabitEthernet1/0/3
ring 2 enable
#
rrpp ring-group 1
domain 2 ring 2
domain 1 ring 3
#
rrpp enable
#

```

- **Device D:**

```

#
vlan 11 to 12
#
stp region-configuration
instance 1 vlan 11
instance 2 vlan 12
active region-configuration
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 11 to 12
port trunk pvid vlan 11
stp disable
qos trust dot1p
#

```

```

interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11 to 12
 port trunk pvid vlan 11
 stp disable
 qos trust dot1p
#
rrpp domain 1
 control-vlan 100
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp domain 2
 control-vlan 105
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp enable
#

```

- **Device E:**

```

#
vlan 12
#
stp region-configuration
 instance 2 vlan 12
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 12
 port trunk pvid vlan 12
 stp disable
 qos trust dot1p
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 12
 port trunk pvid vlan 12

```

```

stp disable
qos trust dot1p
#
rrpp domain 2
control-vlan 105
protected-vlan reference-instance 2
ring 2 node-mode master primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 1
ring 2 enable
#
rrpp enable
#

```

- Device F:

```

#
vlan 11
#
stp region-configuration
instance 1 vlan 11
active region-configuration
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 11
port trunk pvid vlan 11
stp disable
qos trust dot1p
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 11
port trunk pvid vlan 11
stp disable
qos trust dot1p
#
rrpp domain 1
control-vlan 100
protected-vlan reference-instance 1
ring 3 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
ring 3 enable
#
rrpp enable
#

```

# Example: Configuring RRPP and Smart Link

## Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

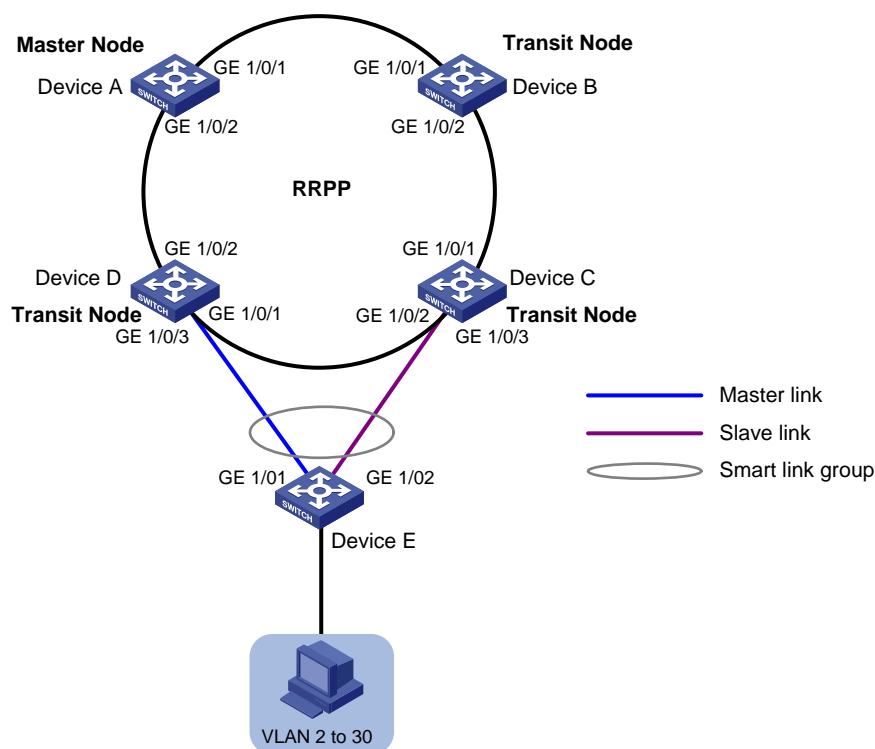
## Network requirements

As shown in [Figure 190](#):

- Device A through Device D support RRPP.
- Device E is a Smart Link device dually uplinked to the distribution layer that adopts a ring topology.

Because Device E at the access layer does not support RRPP, you can use RRPP with Smart Link as a substitution of the RRPP intersecting ring configuration. Configure an RRPP single ring at the distribution layer, and configure Smart Link on the access-layer device. This method ensures high reliability and convergence performance of both the access layer and the distribution layer.

**Figure 190 Network diagram**



## Requirements analysis

For information about configuring a single ring, see "[Example: Configuring single ring.](#)"

## Configuration restrictions and guidelines

When you configure RRPP and Smart Link, follow these restrictions and guidelines:

- For information about configuration restrictions and guidelines for configuring a single ring, see "[Example: Configuring single ring.](#)"
- To prevent loops, shut down a port and then disable the spanning tree feature before configuring it as a smart link group member. You can bring up the port only after completing the smart link group configuration.
- When you configure Device C and Device D, disable the spanning tree feature on the ports that are connected to the member ports of the smart link group. Otherwise, the ports will discard flush messages when they are not in forwarding state if a topology change occurs.
- Make sure the receive control VLAN on Device C and Device D is the same as the transmit control VLAN configured on the Smart Link device. If they are not the same, Device C and Device D might not receive and process flush messages correctly.

## Configuration procedures

### Configuring RRPP single ring

Configure the RRPP single ring on Device A through Device D. For more information, see "[Example: Configuring single ring.](#)"

### Configuring Device E

```
Create VLANs 2 through 30.
<DeviceE> system-view
[DeviceE] vlan 2 to 30
Please wait... Done.

Map these VLANs to MSTI 1.
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 1 vlan 2 to 30

Activate the MST region configuration.
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit

Shut down GigabitEthernet 1/0/1.
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] shutdown

Disable the spanning tree feature on the port.
[DeviceE-GigabitEthernet1/0/1] undo stp enable
```



```

Configure the port as a trunk port.
[DeviceE-GigabitEthernet1/0/1] port link-type trunk

Assign the port to VLANs 2 through 30.
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceE-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2.
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] shutdown
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 2 to 30
Please wait... Done.
[DeviceE-GigabitEthernet1/0/2] quit

Create smart link group 1. Configure all VLANs mapped to MSTI 1 as the protected VLANs.
[DeviceE] smart-link group 1
[DeviceE-smlk-group1] protected-vlan reference-instance 1

Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary
port for smart link group 1.
[DeviceE-smlk-group1] port gigabitethernet 1/0/1 master
[DeviceE-smlk-group1] port gigabitethernet 1/0/2 slave

Enable flush message sending in smart link group 1. Configure VLAN 10 as the transmit control VLAN.
[DeviceE-smlk-group1] flush enable control-vlan 10
[DeviceE-smlk-group1] quit

Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 again.
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo shutdown
[DeviceE-GigabitEthernet1/0/1] quit
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo shutdown
[DeviceE-GigabitEthernet1/0/2] quit

```

## Configuring Device C

```

Disable the spanning tree feature on GigabitEthernet 1/0/3.
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo stp enable

Configure the port as a trunk port.
[DeviceC-GigabitEthernet1/0/3] port link-type trunk

Assign the port to VLANs 2 through 30.
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
Please wait... Done.

Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.
[DeviceC-GigabitEthernet1/0/3] smart-link flush enable control-vlan 10

```

```
[DeviceC-GigabitEthernet1/0/3] quit
```

## Configuring Device D

```
Disable the spanning tree feature on GigabitEthernet 1/0/3.
```

```
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] undo stp enable
```

```
Configure the port as a trunk port.
```

```
[DeviceD-GigabitEthernet1/0/3] port link-type trunk
```

```
Assign the port to VLANs 2 through 30.
```

```
[DeviceD-GigabitEthernet1/0/3] port trunk permit vlan 2 to 30
Please wait... Done.
```

```
Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.
```

```
[DeviceD-GigabitEthernet1/0/3] smart-link flush enable control-vlan 10
[DeviceD-GigabitEthernet1/0/3] quit
```

## Verifying the configuration

1. Use the **display rrpp verbose** command to view RRPP configuration and operational information on each device. For more information, see "[Example: Configuring single ring.](#)"
2. Display the smart link group information:

```
Display the information about smart link group 1 on Device C.
```

```
[DeviceE] display smart-link group 1
Smart link group 1 information:
Device ID: 000f-e23d-5af0
Preemption mode: NONE
Preemption delay: 1(s)
Control VLAN: 10
Protected VLAN: Reference Instance 1
Member Role State Flush-count Last-flush-time

GigabitEthernet1/0/1 MASTER ACTIVE 5 16:37:20 2013/02/21
GigabitEthernet1/0/2 SLAVE STANDBY 1 17:45:20 2013/02/21
```

```
Display the flush messages received on Device D.
```

```
[DeviceD] display smart-link flush
Received flush packets : 5
Receiving interface of the last flush packet : GigabitEthernet1/0/3
Receiving time of the last flush packet : 16:25:21 2013/02/21
Device ID of the last flush packet : 000f-e23d-5af0
Control VLAN of the last flush packet : 10
```

# Configuration files

For information about the RRPP single ring configuration files on Device A through Device D, see ["Example: Configuring single ring."](#)

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device C:

```
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 smart-link flush enable control-vlan 10
#
```

- Device D:

```
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 smart-link flush enable control-vlan 10
#
```

- Device E:

```
#
vlan 2 to 30
#
stp region-configuration
 instance 1 vlan 2 to 30
 active region-configuration
#
smart-link group 1
 protected-vlan reference-instance 1
 flush enable control-vlan 10
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 to 30
 stp disable
 port smart-link group 1 master
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
```

```
port trunk permit vlan 2 to 30
stp disable
port smart-link group 1 slave
#
```

---

# sFlow configuration examples

This chapter provides sFlow configuration examples.

## Example: Configuring sFlow

### Applicable product matrix

| Product series | Software version    |
|----------------|---------------------|
| HP 5500 EI     | Release series 2220 |
| HP 5500 SI     |                     |

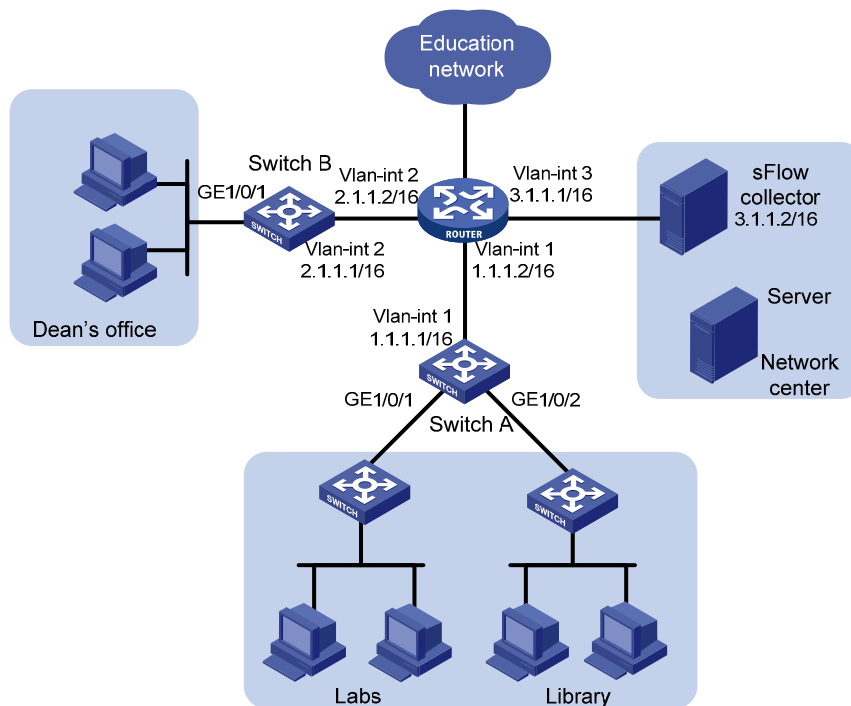
### Network requirements

As shown in [Figure 191](#), configure flow sampling and counter sampling on the following ports to monitor traffic:

- GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch A.
- GigabitEthernet 1/0/1 of Switch B.

Configure Switch A and Switch B to send sampled information in sFlow packets to the sFlow collector that uses the port number 5000.

Figure 191 Network diagram



## Configuration restrictions and guidelines

When you configure sFlow, follow these restrictions and guidelines:

- Set a low sampling rate on the ports with many hosts connected to Switch A. Set a high sampling rate on the port with a few hosts connected to Switch B.
- Set a long counter sampling interval on the ports with many hosts connected to Switch A. Set a short counter sampling interval on the port with a few hosts connected to Switch B.
- Make sure the devices can reach each other before the sFlow configuration.
- Configure the sFlow agents with the same sFlow collector IP address as the remote sFlow collector. Otherwise, the remote sFlow collector cannot receive sFlow packets.

## Configuration procedures

### Configuring Switch A

# Configure the IP address of the sFlow agent.

```
<SwitchA> system-view
[SwitchA] sflow agent ip 1.1.1.1
```

# Configure the sFlow collector ID as **1**, IP address as **3.1.1.2**, and port number as **5000**.

```
[SwitchA] sflow collector 1 ip 3.1.1.2 port 5000
```

# Set the counter sampling interval to **120** seconds. Specify the sFlow collector ID as **1**.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] sflow counter interval 120
[SwitchA-GigabitEthernet1/0/1] sflow counter collector 1
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] sflow counter interval 120
[SwitchA-GigabitEthernet1/0/2] sflow counter collector 1
[SwitchA-GigabitEthernet1/0/2] quit
```

# Set the flow sampling rate to **100000** (one packet is sampled from every 100000 packets). Specify the sFlow collector ID as **1**.

```
[SwitchA-GigabitEthernet1/0/1] sflow sampling-rate 100000
[SwitchA-GigabitEthernet1/0/1] sflow flow collector 1
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] sflow sampling-rate 100000
[SwitchA-GigabitEthernet1/0/2] sflow flow collector 1
[SwitchA-GigabitEthernet1/0/2] quit
```

## Configuring Switch B

# Configure the IP address for the sFlow agent.

```
<SwitchB> system-view
[SwitchB] sflow agent ip 2.1.1.1
```

# Configure the sFlow collector ID as **1**, IP address as **3.1.1.2**, and port number as **5000**.

```
[SwitchB] sflow collector 2 ip 3.1.1.2 port 5000
```

# Set the counter sampling interval to **30** seconds. Specify the sFlow collector ID as **1**.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] sflow counter interval 30
[SwitchB-GigabitEthernet1/0/1] sflow counter collector 1
```

# Set the flow sampling rate to **20000** (one packet is sampled from every 20000 packets). Specify the sFlow collector ID as **1**.

```
[SwitchB-GigabitEthernet1/0/1] sflow sampling-rate 20000
[SwitchB-GigabitEthernet1/0/1] sflow flow collector 1
[SwitchB-GigabitEthernet1/0/1] quit
```

## Verifying the configuration

# Display the sFlow configuration and operation information. This example uses Switch A:

```
[SwitchA] display sflow
sFlow Version: 5
sFlow Global Information:
Agent IP:1.1.1.1(CLI)
Source Address:
Collector Information:
ID IP Port Aging Size VPN-instance Description
1 3.1.1.2 5000 N/A 1400 CLI Collector
```

```

2 6343 0 1400
3 6343 0 1400
4 6343 0 1400
5 6343 0 1400
6 6343 0 1400
7 6343 0 1400
8 6343 0 1400
9 6343 0 1400
10 6343 0 1400

```

sFlow Port Information:

| Interface | CID | Interval(s) | FID | MaxHLen | Rate   | Mode   | Status |
|-----------|-----|-------------|-----|---------|--------|--------|--------|
| GE1/0/1   | 1   | 120         | 1   | 128     | 100000 | Random | Active |
| GE1/0/2   | 1   | 120         | 1   | 128     | 100000 | Random | Active |

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Switch A:

```

#
sflow agent ip 1.1.1.1
sflow collector 1 ip 3.1.1.2 port 5000
#
interface GigabitEthernet1/0/1
port link-mode bridge
sflow sampling-rate 100000
sflow flow collector 1
sflow counter interval 120
sflow counter collector 1
#
interface GigabitEthernet1/0/2
port link-mode bridge
sflow sampling-rate 100000
sflow flow collector 1
sflow counter interval 120
sflow counter collector 1
#

```

- Switch B:

```

#
sflow agent ip 2.1.1.1
sflow collector 1 ip 3.1.1.2 port 5000
#
interface GigabitEthernet1/0/1
port link-mode bridge
sflow sampling-rate 20000
sflow flow collector 1
sflow counter interval 30
sflow counter collector 1

```



#

# Smart Link and CFD collaboration configuration examples

This chapter provides Smart Link and Connectivity Fault Detection (CFD) collaboration configuration examples.

Smart Link supports the Continuity Check (CC) function of CFD to implement link detection. When a fault is detected or cleared, CFD informs Smart Link to switch over the links.

## General configuration restrictions and guidelines

When you configure Smart Link and CFD collaboration, follow these restrictions and guidelines:

- Disable the spanning tree feature and RRPP on the ports that you want to add to a smart link group.
- Make sure the ports are not member ports of any aggregation group or service loopback group.

## Example: Single smart link group and CFD collaboration configuration example

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

### Network requirements

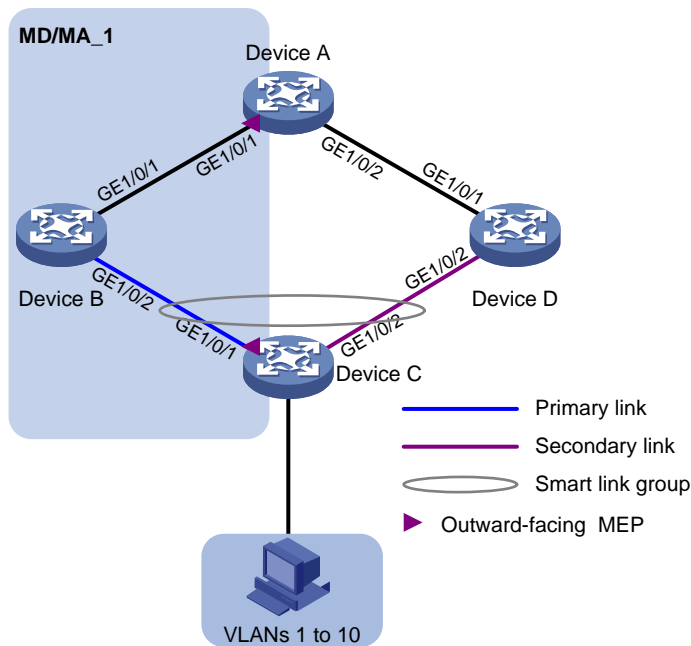
As shown in [Figure 192](#), traffic of VLANs 1 through 10 on Device C is dually uplinked to Device A by Device B and Device D.

Configure Smart Link and CFD collaboration on Device C, and configure CFD on Device C and Device A to meet the following requirements:

- User traffic is forwarded through the primary port of the smart link group on Device C.
- When the link between the primary port and Device A fails, the secondary port of the smart link group immediately transits to forwarding state.

- When the link between the primary port and Device A recovers, the primary port of the smart link group transits to forwarding state.

**Figure 192 Network diagram**



## Requirements analysis

In this example, to enable Device C to prefer Device B to forward user traffic to Device A, configure GigabitEthernet 1/0/1 as the primary port of the smart link group on Device C.

To make sure the primary port of the smart link group immediately transits to forwarding state when the primary link recovers, configure role preemption for the smart link group.

## Configuration restrictions and guidelines

When you configure single smart link group and CFD collaboration, follow these restrictions and guidelines:

- Before you configure a port as a smart link group member, shut down the port to prevent loops. You can bring up the port only after completing the smart link group configuration.
- Disable the spanning tree feature on the associated device's ports that connect to the member ports of the smart link group. Otherwise, the ports will discard flush messages if they are not in the forwarding state when a topology change occurs.
- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.

- Make sure the receive control VLAN is the same as the transmit control VLAN configured on the Smart Link device. If they are not the same, the associated device will forward the received flush messages without any processing.
- Make sure the control VLAN of the smart link group matches the detection VLAN of the CC function of CFD.

## Configuration procedures

### Configuring Device C

1. Configure VLAN and MST region settings:

# Create VLAN 1 through VLAN 10.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 10
Please wait... Done.
```

# Map these VLANs to MSTI 0.

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 0 vlan 1 to 10
```

# Activate MST region configuration.

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

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

# Shut down GigabitEthernet 1/0/1.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
```

# Disable the spanning tree feature on the port.

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

# Configure the port as a trunk port. Assign the port to VLAN 1 through VLAN 10.

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 10
Please wait... Done.
```

```
[DeviceC-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/1] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 10
Please wait... Done.
[DeviceC-GigabitEthernet1/0/2] quit
```

3. Configure smart link group 1:

# Create smart link group 1.

```
[DeviceC] smart-link group 1
```

```

Configure all VLANs mapped to MSTI 0 as the protected VLANs.
[DeviceC-smlk-group1] protected-vlan reference-instance 0

Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the
secondary port for smart link group 1.
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 master
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 slave

Enable role preemption in smart link group 1.
[DeviceC-smlk-group1] preemption mode role

Enable flush update for smart link group 1. Specify VLAN 10 as the control VLAN.
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit

Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit

```

#### 4. Configure CFD:

```

Enable CFD.
<DeviceC> system-view
[DeviceC] cfd enable

Create service instance 1 in which the MA serves VLAN 10.
[DeviceC] cfd md MD level 5
[DeviceC] cfd ma MA_1 md MD vlan 10
[DeviceC] cfd service-instance 1 md MD ma MA_1

Configure MEPS.
[DeviceC] cfd meplist 1001 1002 service-instance 1
[DeviceC] interface GigabitEthernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 outbound
[DeviceC-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1001 enable

Enable the sending of CCM frames for MEP 1001 in service instance 1 on GigabitEthernet
1/0/1.
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceC-GigabitEthernet1/0/1] quit

```

### Configuring Device B

1. Create VLAN 1 through VLAN 10.

```

<DeviceB> system-view
[DeviceB] vlan 1 to 10
Please wait... Done.

```
2. Configure GigabitEthernet 1/0/1:

```

Configure GigabitEthernet 1/0/1 as a trunk port. Assign it to VLANs 1 through 10.

```

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 10
Please wait... Done.
```

# Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.

```
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10
[DeviceB-GigabitEthernet1/0/1] quit
```

### 3. Configure GigabitEthernet 1/0/2:

# Configure GigabitEthernet 1/0/2 as a trunk port. Assign it to VLANs 1 through 10.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 10
Please wait... Done.
```

# Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/2] undo stp enable
```

# Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.

```
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10
[DeviceB-GigabitEthernet1/0/2] quit
```

## Configuring Device D

### 1. Create VLAN 1 through VLAN 10.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 10
Please wait... Done.
```

### 2. Configure GigabitEthernet 1/0/1:

# Configure GigabitEthernet 1/0/1 as a trunk port. Assign it to VLANs 1 through 10.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 10
Please wait... Done.
```

# Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.

```
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10
[DeviceD-GigabitEthernet1/0/1] quit
```

### 3. Configure GigabitEthernet 1/0/2:

# Configure GigabitEthernet 1/0/2 as a trunk port. Assign it to VLANs 1 through 10.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 10
Please wait... Done.
```

# Disable the spanning tree feature on the port.

```
[DeviceD-GigabitEthernet1/0/2] undo stp enable
```

# Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.

```
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10
[DeviceD-GigabitEthernet1/0/2] quit
```

## Configuring Device A

1. Create VLAN 1 through VLAN 10.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 10
Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

# Configure GigabitEthernet 1/0/1 as a trunk port. Assign it to VLANs 1 through 10.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 10
Please wait... Done.
```

# Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.

```
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10
[DeviceA-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 10
Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10
[DeviceA-GigabitEthernet1/0/2] quit
```

3. Configure CFD:

# Enable CFD.

```
<DeviceA> system-view
[DeviceA] cfd enable
```

# Create service instance 1, in which the MA serves VLAN 10.

```
[DeviceA] cfd md MD level 5
[DeviceA] cfd ma MA_1 md MD vlan 10
[DeviceA] cfd service-instance 1 md MD ma MA_1
```

# Configure MEPS.

```
[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1002 enable
```

# Enable the sending of CCM frames for MEP 1002 in service instance 1 on GigabitEthernet 1/0/1.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

## Configuring the collaboration between Smart Link and the CC function of CFD

# Configure the collaboration between Smart Link and the CC function of CFD on Device C.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port smart-link group 1 track cfd cc
```

```
[DeviceC-GigabitEthernet1/0/1] quit
```

## Verifying the configuration

# After you shut down GigabitEthernet 1/0/1 on Device B, use the **display smart-link group** command to display the smart link group configuration on Device C.

```
[DeviceC] display smart-link group all
Smart link group 1 information:
Device ID: 0023-895f-954f
Preemption mode: ROLE
Preemption delay: 1(s)
Control VLAN: 10
Protected VLAN: Reference Instance 0
Member Role State Flush-count Last-flush-time

GigabitEthernet1/0/1 MASTER DOWN 0 NA
GigabitEthernet1/0/2 SLAVE ACTIVE 1 14:32:56 2012/12/11
```

The output shows the following:

- Primary port GigabitEthernet 1/0/1 of smart link group 1 fails.
- Secondary port GigabitEthernet 1/0/2 is in forwarding state.
- A link switchover occurs.

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```
#
 cfd enable
 cfd md MD level 5
 cfd ma MA_1 md MD vlan 10
 cfd service-instance 1 md MD ma MA_1
 cfd meplist 1001 to 1002 service-instance 1
#
vlan 1
#
vlan 2 to 10
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 10
 smart-link flush enable control-vlan 10
 cfd mep 1002 service-instance 1 outbound
```



```

cfd mep service-instance 1 mep 1002 enable
cfd cc service-instance 1 mep 1002 enable
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 10
smart-link flush enable control-vlan 10
#

```

- **Device B:**

```

#
vlan 1
#
vlan 2 to 10
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 10
smart-link flush enable control-vlan 10
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 10
stp disable
smart-link flush enable control-vlan 10
#

```

- **Device C:**

```

#
cfd enable
cfd md MD level 5
cfd ma MA_1 md MD vlan 10
cfd service-instance 1 md MD ma MA_1
cfd meplist 1001 to 1002 service-instance 1
#
vlan 1
#
vlan 2 to 10
#
stp region-configuration
instance 0 vlan 1 to 10
active region-configuration
#
smart-link group 1
preemption mode role
protected-vlan reference-instance 0
flush enable control-vlan 10

```

```

#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 10
 stp disable
 port smart-link group 1 master
 port smart-link group 1 track cfd cc
 cfd mep 1001 service-instance 1 outbound
 cfd mep service-instance 1 mep 1001 enable
 cfd cc service-instance 1 mep 1001 enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 10
 stp disable
 port smart-link group 1 slave
#

```

- Device D:

```

#
vlan 1
#
vlan 2 to 10
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 10
 smart-link flush enable control-vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 10
 stp disable
 smart-link flush enable control-vlan 10
#

```

# Example: Multiple smart link groups and CFD collaboration configuration example

## Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

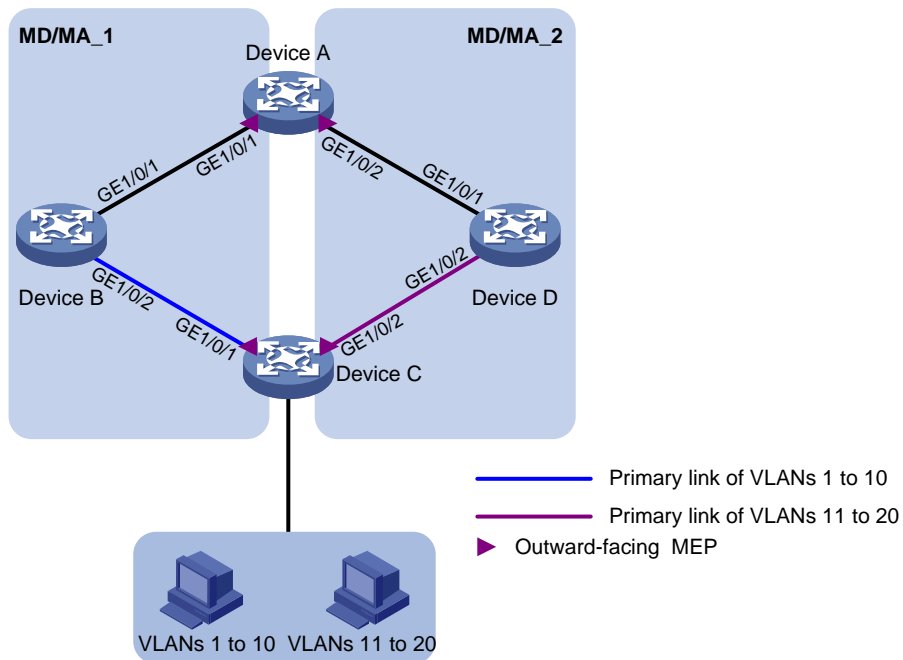
## Network requirements

As shown in [Figure 193](#), traffic of VLANs 1 through 20 on Device C is dually uplinked to Device A by Device B and Device D.

Configure multiple smart link groups and CFD collaboration on Device C, and configure CFD on Device C and Device A to meet the following requirements:

- Traffic of VLANs 1 through 10 is uplinked to Device A by Device B. Traffic of VLANs 11 through 20 is uplinked to Device A by Device D.
- When the links between primary ports of the smart link groups and Device A fail, the secondary ports immediately transit to forwarding state.
- When the links between the primary ports and Device A recover, the primary ports of the smart link groups transit to forwarding state. Traffic load sharing is implemented.

Figure 193 Network diagram



## Requirements analysis

In this example, to enable Device C to forward traffic of VLANs 1 through 10 through Device B and traffic of VLANs 11 through 20 through Device D, do the following:

- Configure GigabitEthernet 1/0/1 as the primary port for smart link group 1.
- Configure GigabitEthernet 1/0/2 as the primary port for smart link group 2 on Device C.

To make sure the primary port of the smart link group immediately transits to forwarding state when the primary link recovers, configure role preemption for the smart link group.

## Configuration restrictions and guidelines

When you configure multiple smart link groups and CFD collaboration, follow these restrictions and guidelines:

- Before you configure a port as a smart link group member, shut down the port to prevent loops. You can bring up the port only after completing the smart link group configuration.
- Disable the spanning tree feature on the associated device's ports that connect to the member ports of the smart link group. Otherwise, the ports will discard flush messages if they are not in the forwarding state when a topology change occurs.
- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.

- Make sure the receive control VLAN is the same as the transmit control VLAN configured on the Smart Link device. If they are not the same, the associated device will forward the received flush messages without any processing.
- Make sure the control VLAN of the smart link group matches the detection VLAN of the CC function of CFD.

## Configuration procedures

### Configuring Device C

1. Configure VLAN and MST region settings:

```
Create VLAN 1 through VLAN 20.
```

```
<DeviceC> system-view
[DeviceC] vlan 1 to 20
Please wait... Done.
```

```
Map VLANs 1 through 10 to MSTI 0, and VLANs 11 through 20 to MSTI 1.
```

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 0 vlan 1 to 10
[DeviceC-mst-region] instance 1 vlan 11 to 20
```

```
Activate MST region configuration.
```

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

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

```
Shut down GigabitEthernet 1/0/1.
```

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
```

```
Disable the spanning tree feature on the port.
```

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

```
Configure the port as a trunk port. Assign the port to VLAN 1 through VLAN 20.
```

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
Please wait... Done.
[DeviceC-GigabitEthernet1/0/1] quit
```

```
Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
```

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
Please wait... Done.
[DeviceC-GigabitEthernet1/0/2] quit
```

3. Configure smart link group 1:

```
Create smart link group 1.
```

```

[DeviceC] smart-link group 1
Configure all VLANs mapped to MSTI 0 as the protected VLANs for smart link group 1.
[DeviceC-smlk-group1] protected-vlan reference-instance 0
Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the
secondary port for smart link group 1.
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 master
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 slave
Enable role preemption in smart link group 1.
[DeviceC-smlk-group1] preemption mode role
Enable flush update for smart link group 1. Specify VLAN 10 as the control VLAN.
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit

```

#### 4. Configure smart link group 2:

```

Create smart link group 2.
[DeviceC] smart-link group 2
Configure all VLANs mapped to MSTI 1 as the protected VLANs for smart link group 2.
[DeviceC-smlk-group2] protected-vlan reference-instance 1
Configure GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the
secondary port for smart link group 2.
[DeviceC-smlk-group2] port gigabitethernet 1/0/2 master
[DeviceC-smlk-group2] port gigabitethernet 1/0/1 slave
Enable role preemption in smart link group 2.
[DeviceC-smlk-group2] preemption mode role
Enable flush update for smart link group 2. Specify VLAN 20 as the control VLAN.
[DeviceC-smlk-group2] flush enable control-vlan 20
[DeviceC-smlk-group2] quit
Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit

```

#### 5. Configure CFD:

```

Enable CFD.
<DeviceC> system-view
[DeviceC] cfd enable
Create service instance 1, in which the MA serves VLAN 10.
[DeviceC] cfd md MD level 5
[DeviceC] cfd ma MA_1 md MD vlan 10
[DeviceC] cfd service-instance 1 md MD ma MA_1
Create service instance 2, in which the MA serves VLAN 20.

```

```

[DeviceC] cfd ma MA_2 md MD vlan 20
[DeviceC] cfd service-instance 2 md MD ma MA_2

Configure MEPS.
[DeviceC] cfd meplist 1001 1002 service-instance 1
[DeviceC] cfd meplist 2001 2002 service-instance 2
[DeviceC] interface GigabitEthernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 outbound
[DeviceC-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1001 enable
[DeviceC-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 outbound
[DeviceC-GigabitEthernet1/0/2] cfd mep service-instance 2 mep 2001 enable

Enable the sending of CCM frames for MEPS.
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceC-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceC-GigabitEthernet1/0/2] quit

```

## Configuring Device B

### 1. Create VLAN 1 through VLAN 20.

```

<DeviceB> system-view
[DeviceB] vlan 1 to 20
Please wait... Done.

```

### 2. Configure GigabitEthernet 1/0/1:

# Configure GigabitEthernet 1/0/1 as a trunk port. Assign it to VLANs 1 through 20.

```

[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
Please wait... Done.

```

# Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```

[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit

```

### 3. Configure GigabitEthernet 1/0/2:

# Configure GigabitEthernet 1/0/2 as a trunk port. Assign it to VLANs 1 through 20.

```

[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
Please wait... Done.

```

# Disable the spanning tree feature on the port.

```

[DeviceB-GigabitEthernet1/0/2] undo stp enable

```

# Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```

[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/2] quit

```

## Configuring Device D

1. Create VLAN 1 through VLAN 20.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 20
Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1:

# Configure GigabitEthernet 1/0/1 as a trunk port. Assign it to VLANs 1 through 20.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
Please wait... Done.
```

# Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceD-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

# Configure GigabitEthernet 1/0/2 as a trunk port. Assign it to VLANs 1 through 20.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
Please wait... Done.
```

# Disable the spanning tree feature.

```
[DeviceD-GigabitEthernet1/0/2] undo stp enable
```

# Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceD-GigabitEthernet1/0/2] quit
```

## Configuring Device A

1. Create VLAN 1 through VLAN 20.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 20
Please wait... Done.
```

2. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

# Configure GigabitEthernet 1/0/1 as a trunk port. Assign the port to VLAN 1 through VLAN 20.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
Please wait... Done.
```

# Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/1] quit
```



# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/2] quit
```

### 3. Configure CFD:

# Enable CFD.

```
<DeviceA> system-view
[DeviceA] cfd enable
```

# Create service instance 1, in which the MA serves VLAN 10.

```
[DeviceA] cfd md MD level 5
[DeviceA] cfd ma MA_1 md MD vlan 10
[DeviceA] cfd service-instance 1 md MD ma MA_1
```

# Create service instance 2, in which the MA serves VLAN 20.

```
[DeviceA] cfd ma MA_2 md MD vlan 20
[DeviceA] cfd service-instance 2 md MD ma MA_2
```

# Configure MEPS.

```
[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] cfd meplist 2001 2002 service-instance 2
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1002 enable
[DeviceA-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd mep 2002 service-instance 2 outbound
[DeviceA-GigabitEthernet1/0/2] cfd mep service-instance 2 mep 2002 enable
```

# Enable the sending of CCM frames for MEPS.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceA-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2002 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

## Configuring the collaboration between Smart Link and the CC function of CFD

# Configure the collaboration between Smart Link and the CC function of CFD on Device C.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port smart-link group 1 track cfd cc
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port smart-link group 2 track cfd cc
```

## Verifying the configuration

# After you shut down GigabitEthernet 1/0/1 on Device B, use the **display smart-link group** command to display the smart link group configuration on Device C.

```
[DeviceC] display smart-link group all
Smart link group 1 information:
Device ID: 0023-895f-954f
Preemption mode: ROLE
Preemption delay: 1(s)
Control VLAN: 10
Protected VLAN: Reference Instance 0
Member Role State Flush-count Last-flush-time

GigabitEthernet1/0/1 MASTER DOWN 0 NA
GigabitEthernet1/0/2 SLAVE ACTIVE 1 14:32:56 2012/12/11

Smart link group 2 information:
Device ID: 0023-895f-954f
Preemption mode: ROLE
Preemption delay: 1(s)
Control VLAN: 20
Protected VLAN: Reference Instance 1
Member Role State Flush-count Last-flush-time

GigabitEthernet1/0/2 MASTER ACTIVE 0 NA
GigabitEthernet1/0/1 SLAVE DOWN 0 NA
```

The output shows the following:

- Primary port GigabitEthernet 1/0/1 of smart link group 1 fails.
- Secondary port GigabitEthernet 1/0/2 is in forwarding state.
- A link switchover occurs.

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```
#
cfd enable
cfd md MD level 5
cfd ma MA_1 md MD vlan 10
cfd service-instance 1 md MD ma MA_1
cfd meplist 1001 to 1002 service-instance 1
cfd ma MA_2 md MD vlan 20
cfd service-instance 2 md MD ma MA_2
cfd meplist 2001 to 2002 service-instance 2
```

```

#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 20
smart-link flush enable control-vlan 10 20
cfd mep 1002 service-instance 1 outbound
cfd mep service-instance 1 mep 1002 enable
cfd cc service-instance 1 mep 1002 enable
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 20
smart-link flush enable control-vlan 10 20
cfd mep 2002 service-instance 2 outbound
cfd mep service-instance 2 mep 2002 enable
cfd cc service-instance 2 mep 2002 enable
#

```

- **Device B:**

```

#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 20
smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 20
stp disable
smart-link flush enable control-vlan 10 20
#

```

- **Device C:**

```

#
cfd enable
cfd md MD level 5
cfd ma MA_1 md MD vlan 10
cfd service-instance 1 md MD ma MA_1

```

```

cfd meplist 1001 to 1002 service-instance 1
cfd ma MA_2 md MD vlan 20
cfd service-instance 2 md MD ma MA_2
cfd meplist 2001 to 2002 service-instance 2
#
vlan 1
#
vlan 2 to 20
#
stp region-configuration
instance 0 vlan 1 to 10
instance 1 vlan 11 to 20
active region-configuration
#
smart-link group 1
preemption mode role
protected-vlan reference-instance 0
flush enable control-vlan 10
smart-link group 2
preemption mode role
protected-vlan reference-instance 1
flush enable control-vlan 20
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 20
stp disable
port smart-link group 1 master
port smart-link group 1 track cfd cc
port smart-link group 2 slave
cfd mep 1001 service-instance 1 outbound
cfd mep service-instance 1 mep 1001 enable
cfd cc service-instance 1 mep 1001 enable
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 20
stp disable
port smart-link group 1 slave
port smart-link group 2 master
port smart-link group 2 track cfd cc
cfd mep 2001 service-instance 2 outbound
cfd mep service-instance 2 mep 2001 enable
cfd cc service-instance 2 mep 2001 enable
#

```

- Device D:

```
#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 smart-link flush enable control-vlan 10 20
#
```

# Smart Link configuration examples

This chapter provides Smart Link configuration examples.

Smart Link provides link redundancy as well as fast convergence in a dual uplink network, allowing the backup link to take over quickly when the primary link fails.

## General configuration restrictions and guidelines

Disable the spanning tree feature and RRPP on the ports that you want to add to a smart link group, and make sure the ports are not member ports of any aggregation group or service loopback group.

## Example: Configuring single smart link group

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

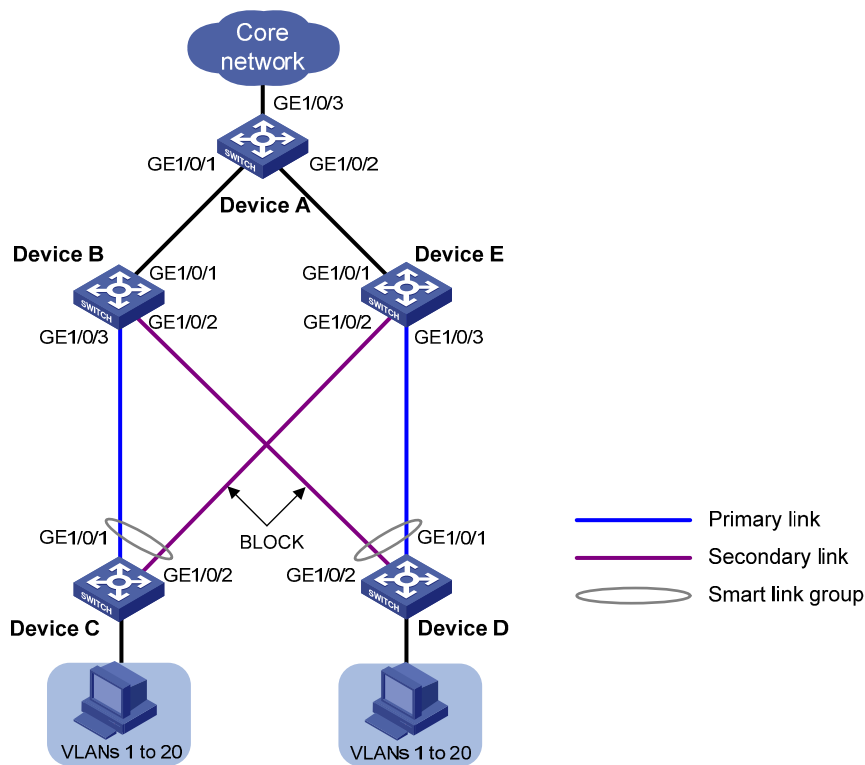
As shown in [Figure 194](#), Device C and Device D:

- Are each connected to a user network consisting of VLANs 1 through 20.
- Are dually uplinked to Device A through Device B and Device E.

Configure Smart Link on Device C and Device D to meet the following requirements:

- Enable Device C to prefer Device B, and Device D to prefer Device E to forward user traffic to Device A.
- When one forwarding link fails, user traffic is immediately switched to another link to implement dual uplink backup.

Figure 194 Network diagram



## Requirements analysis

In this example, to enable Device C to prefer Device B, and Device D to prefer Device E to forward user traffic to Device A, configure GigabitEthernet 1/0/1 as the primary port of the smart link group on Device C and Device D.

## Configuration restrictions and guidelines

When you configure a single smart link group, follow these restrictions and guidelines:

- Before you configure a port as a smart link group member, shut down the port to prevent loops. You can bring up the port only after completing the smart link group configuration.
- Disable the spanning tree feature on the associated device's ports that connect to the member ports of the smart link group. Otherwise, the ports will discard flush messages when they are not in the forwarding state if a topology change occurs.
- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.
- Make sure the receive control VLAN configured on the associated device is the same as the transmit control VLAN configured on the Smart Link device. If they are not the same, the associated device will forward the received flush messages without any processing.

# Configuration procedures

## Configuring Device C

# Create VLAN 1 through VLAN 20.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 20
Please wait... Done.
```

# Map these VLANs to MSTI 1.

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 20
```

# Activate MST region configuration.

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

# Shut down GigabitEthernet 1/0/1.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
```

# Disable the spanning tree feature on the port.

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

# Configure the port as a trunk port.

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

# Assign the port to VLAN 1 through VLAN 20.

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
Please wait... Done.
[DeviceC-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
Please wait... Done.
[DeviceC-GigabitEthernet1/0/2] quit
```

# Create smart link group 1. Configure all VLANs mapped to MSTI 1 as the protected VLANs for smart link group 1.

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

# Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port for smart link group 1.

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 master
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 slave
```

# Enable flush message sending in smart link group 1. Configure VLAN 10 as the transmit control VLAN.



```
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit
```

**# Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 again.**

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

## Configuring Device D

**# Create VLAN 1 through VLAN 20.**

```
<DeviceD> system-view
[DeviceD] vlan 1 to 20
Please wait... Done.
```

**# Map these VLANs to MSTI 1.**

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 20
```

**# Activate MST region configuration.**

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

**# Shut down GigabitEthernet 1/0/1.**

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] shutdown
```

**# Disable the spanning tree feature on the port.**

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

**# Configure the port as a trunk port.**

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

**# Assign the port to VLAN 1 through VLAN 20.**

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
Please wait... Done.
[DeviceD-GigabitEthernet1/0/1] quit
```

**# Configure GigabitEthernet 1/0/2.**

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] shutdown
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
Please wait... Done.
[DeviceD-GigabitEthernet1/0/2] quit
```

**# Create smart link group 1. Configure all VLANs mapped to MSTI 1 as the protected VLANs for smart link group 1.**

```
[DeviceD] smart-link group 1
```

```

[DeviceD-smlk-group1] protected-vlan reference-instance 1

Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary
port for smart link group 1.
[DeviceD-smlk-group1] port gigabitethernet 1/0/1 master
[DeviceD-smlk-group1] port gigabitethernet 1/0/2 slave

Enable flush message sending in smart link group 1. Configure VLAN 20 as the transmit control VLAN.
[DeviceD-smlk-group1] flush enable control-vlan 20
[DeviceD-smlk-group1] quit

Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 again.
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] quit

```

## Configuring Device B

```

Create VLAN 1 through VLAN 20.
<DeviceB> system-view
[DeviceB] vlan 1 to 20
Please wait... Done.

Configure GigabitEthernet 1/0/1 as a trunk port.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk

Assign the port to VLAN 1 through VLAN 20.
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
Please wait... Done.

Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control
VLANs.
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2 as a trunk port.
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk

Assign the port to VLAN 1 through VLAN 20.
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
Please wait... Done.

Disable the spanning tree feature on the port.
[DeviceB-GigabitEthernet1/0/2] undo stp enable

Enable flush message receiving on the port. Configure VLAN 20 as the receive control VLAN.
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 20
[DeviceB-GigabitEthernet1/0/2] quit

```

```

Configure GigabitEthernet 1/0/3 as a trunk port.
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk

Assign the port to VLAN 1 through VLAN 20.
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 20
Please wait... Done.

Disable the spanning tree feature on the port.
[DeviceB-GigabitEthernet1/0/3] undo stp enable

Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.
[DeviceB-GigabitEthernet1/0/3] smart-link flush enable control-vlan 10
[DeviceB-GigabitEthernet1/0/3] quit

```

## Configuring Device E

```

Create VLAN 1 through VLAN 20.
<DeviceE> system-view
[DeviceE] vlan 1 to 20
Please wait... Done.

Configure GigabitEthernet 1/0/1 as a trunk port.
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] port link-type trunk

Assign the port to VLAN 1 through VLAN 20.
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
Please wait... Done.

Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.
[DeviceE-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceE-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2 as a trunk port.
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] port link-type trunk

Assign the port to VLAN 1 through VLAN 20.
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
Please wait... Done.

Disable the spanning tree feature on the port.
[DeviceE-GigabitEthernet1/0/2] undo stp enable

Enable flush message receiving on the port. Configure VLAN 10 as the receive control VLAN.
[DeviceE-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10
[DeviceE-GigabitEthernet1/0/2] quit

Configure GigabitEthernet 1/0/3 as a trunk port.
[DeviceE] interface gigabitethernet 1/0/3
[DeviceE-GigabitEthernet1/0/3] port link-type trunk

Assign the port to VLAN 1 through VLAN 20.

```

```
[DeviceE-GigabitEthernet1/0/3] port trunk permit vlan 1 to 20
Please wait... Done.

Disable the spanning tree feature on the port.
[DeviceE-GigabitEthernet1/0/2] undo stp enable

Enable flush message receiving on the port. Configure VLAN 20 as the receive control VLAN.
[DeviceE-GigabitEthernet1/0/3] smart-link flush enable control-vlan 20
[DeviceE-GigabitEthernet1/0/3] quit
```

## Configuring Device A

```
Create VLAN 1 through VLAN 20.
<DeviceA> system-view
[DeviceA] vlan 1 to 20
Please wait... Done.

Configure GigabitEthernet 1/0/1 as a trunk port.
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk

Assign the port to VLAN 1 through VLAN 20.
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
Please wait... Done.

Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2.
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/2] quit
```

## Verifying the configuration

# Use the **display smart-link group** command to display the smart link group configuration on Device C.

```
[DeviceC] display smart-link group 1
Smart link group 1 information:
Device ID: 000f-e23d-5af0
Preemption mode: NONE
Preemption delay: 1(s)
Control VLAN: 10
Protected VLAN: Reference Instance 1
Member Role State Flush-count Last-flush-time

GigabitEthernet1/0/1 MASTER ACTIVE 2 18:37:20 2013/02/21
```

```
GigabitEthernet1/0/2 SLAVE STANDBY 2 17:45:20 2013/02/21
```

The output shows that GigabitEthernet 1/0/1 on Device C becomes active to forward user traffic after multiple uplink switchovers.

# Use the **display smart-link flush** command to display the flush messages received on Device B.

```
[DeviceB] display smart-link flush
Received flush packets : 2
Receiving interface of the last flush packet : GigabitEthernet1/0/3
Receiving time of the last flush packet : 18:37:21 2013/02/21
Device ID of the last flush packet : 000f-e23d-5af0
Control VLAN of the last flush packet : 10
```

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```
#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 20
smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 20
smart-link flush enable control-vlan 10 20
#
```

- Device B:

```
#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 20
smart-link flush enable control-vlan 10 20
#
```

```

interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 smart-link flush enable control-vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 smart-link flush enable control-vlan 10
#

```

- Device C:

```

#
vlan 1
#
vlan 2 to 20
#
stp region-configuration
 instance 1 vlan 1 to 20
 active region-configuration
#
smart-link group 1
 protected-vlan reference-instance 1
 flush enable control-vlan 10
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 port smart-link group 1 master
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 port smart-link group 1 slave
#

```

- Device D:

```

#
vlan 1
#
vlan 2 to 20
#

```

```

stp region-configuration
 instance 1 vlan 1 to 20
 active region-configuration
#
smart-link group 1
 protected-vlan reference-instance 1
 flush enable control-vlan 20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 port smart-link group 1 master
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 port smart-link group 1 slave
#

```

- **Device E:**

```

#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 smart-link flush enable control-vlan 10
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 smart-link flush enable control-vlan 20
#

```

# Example: Configuring multi-smart link group load sharing

## Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

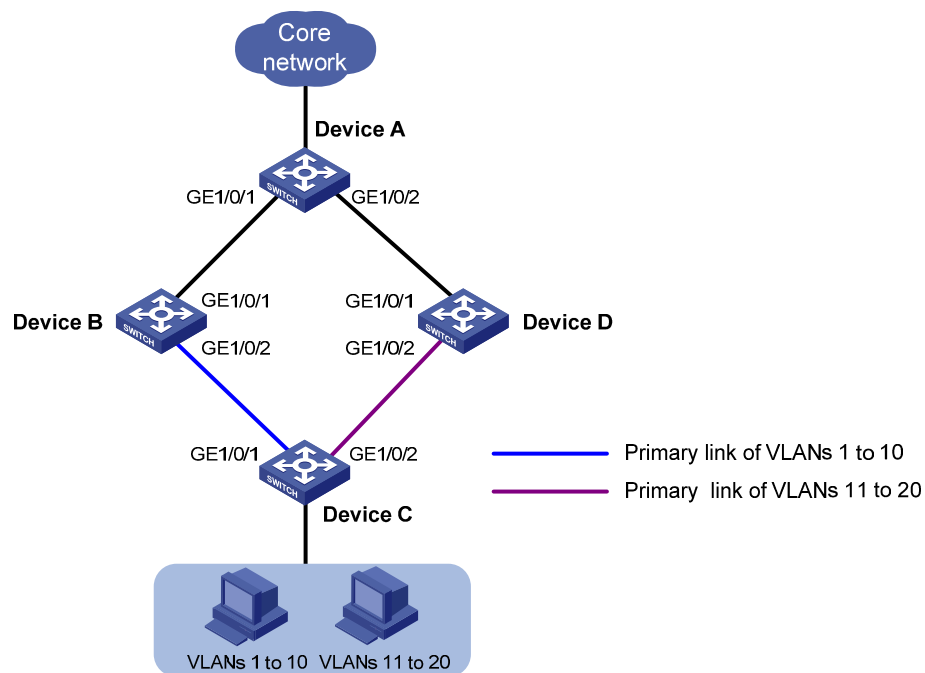
As shown in [Figure 195](#), traffic of VLANs 1 through 20 on Device C is dually uplinked to Device A by Device B and Device D.

Configure multiple smart link groups on Device C to meet the following requirements:

- Traffic of VLANs 1 through 10 is uplinked to Device A by Device B. Traffic of VLANs 11 through 20 is uplinked to Device A by Device D.
- When the primary link of a smart link group fails, the secondary link immediately takes over to forward user traffic to implement dual uplink backup.
- When the primary link recovers, user traffic is immediately switched back to the primary link of the smart link group. Both links forward user traffic to implement load sharing.



Figure 195 Network diagram



## Requirements analysis

In this example, to enable Device C to forward traffic of VLANs 1 through 10 through Device B and traffic of VLANs 11 through 20 through Device D, do the following:

- Configure GigabitEthernet 1/0/1 as the primary port for smart link group 1.
- Configure GigabitEthernet 1/0/2 as the primary port for smart link group 2 on Device C.

To make sure user traffic can be switched back to the primary link of a smart link group when the link recovers from a failure, enable role preemption for both smart link groups.

## Configuration restrictions and guidelines

When you configure multi-smart link group load sharing, follow these restrictions and guidelines:

- Before you configure a port as a smart link group member, shut down the port to prevent loops. You can bring up the port only after completing the smart link group configuration.
- Disable the spanning tree feature on the associated device's ports that connect to the member ports of the smart link group. Otherwise, the ports will discard flush messages when they are not in the forwarding state if a topology change occurs.
- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.

- Make sure the receive control VLAN configured on the associated device is the same as the transmit control VLAN configured on the Smart Link device. If they are not the same, the associated device will forward the received flush messages without any processing.

## Configuration procedures

### Configuring Device C

# Create VLAN 1 through VLAN 20.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 20
Please wait... Done.
```

# Map VLANs 1 through 10 to MSTI 1, and VLANs 11 through 20 to MSTI 2.

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 10
[DeviceC-mst-region] instance 2 vlan 11 to 20
```

# Activate MST region configuration.

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

# Shut down GigabitEthernet 1/0/1.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
```

# Disable the spanning tree feature on the port.

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

# Configure the port as a trunk port.

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

# Assign the port to VLAN 1 through VLAN 20.

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
Please wait... Done.
[DeviceC-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
Please wait... Done.
[DeviceC-GigabitEthernet1/0/2] quit
```

# Create smart link group 1. Configure all VLANs mapped to MSTI 1 as the protected VLANs for smart link group 1.

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

# Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port for smart link group 1.

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 master
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 slave
```

# Enable role preemption in smart link group 1.

```
[DeviceC-smlk-group1] preemption mode role
```

# Enable flush message sending. Configure VLAN 10 as the transmit control VLAN.

```
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit
```

# Create smart link group 2. Configure all VLANs mapped to MSTI 2 as the protected VLANs for smart link group 2.

```
[DeviceC] smart-link group 2
[DeviceC-smlk-group2] protected-vlan reference-instance 2
```

# Configure GigabitEthernet 1/0/1 as the secondary port and GigabitEthernet 1/0/2 as the primary port for smart link group 2.

```
[DeviceC-smlk-group2] port gigabitethernet 1/0/2 master
[DeviceC-smlk-group2] port gigabitethernet 1/0/1 slave
```

# Enable role preemption in smart link group 2.

```
[DeviceC-smlk-group2] preemption mode role
```

# Enable flush message sending. Configure VLAN 20 as the transmit control VLAN.

```
[DeviceC-smlk-group2] flush enable control-vlan 20
[DeviceC-smlk-group2] quit
```

# Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 again.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

## Configuring Device B

# Create VLAN 1 through VLAN 20.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 20
Please wait... Done.
```

# Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

# Assign the port to VLAN 1 through VLAN 20.

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
Please wait... Done.
```

# Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 as a trunk port.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
```

# Assign the port to VLAN 1 through VLAN 20.

```
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
Please wait... Done.
```

# Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/2] undo stp enable
```

# Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/2] quit
```

## Configuring Device D

# Create VLAN 1 through VLAN 20.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 20
Please wait... Done.
```

# Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

# Assign the port to VLAN 1 through VLAN 20.

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
Please wait... Done.
```

# Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceD-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 as a trunk port.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
```

# Assign the port to VLAN 1 through VLAN 20.

```
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
Please wait... Done.
```

# Disable the spanning tree feature on the port.

```
[DeviceD-GigabitEthernet1/0/2] undo stp enable
```

# Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceD-GigabitEthernet1/0/2] quit
```

## Configuring Device A

# Create VLAN 1 through VLAN 20.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 20
Please wait... Done.
```

# Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

# Assign the port to VLAN 1 through VLAN 20.

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 20
Please wait... Done.
```

# Enable flush message receiving on the port. Configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 20
Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/2] quit
```

## Verifying the configuration

# Shut down GigabitEthernet 1/0/1 on Device C. Display the smart link group configuration on Device C.

```
[DeviceC] display smart-link group all
Smart link group 1 information:
Device ID: 000f-e23d-5af0
Preemption mode: ROLE
Preemption delay: 1(s)
Control VLAN: 10
Protected VLAN: Reference Instance 1
Member Role State Flush-count Last-flush-time

GigabitEthernet1/0/1 MASTER DOWN 0 NA
GigabitEthernet1/0/2 SLAVE ACTIVE 1 17:45:20 2013/02/21

Smart link group 2 information:
```

```

Device ID: 000f-e23d-5af0
Preemption mode: ROLE
Preemption delay: 1(s)
Control VLAN: 20
Protected VLAN: Reference Instance 2
Member Role State Flush-count Last-flush-time

GigabitEthernet1/0/2 MASTER ACTIVE 0 NA
GigabitEthernet1/0/1 SLAVE DOWN 0 NA

```

The output shows that:

- A link switchover occurs in smart link group 1.
- No link switchover occurs in smart link group 2.

# Bring up GigabitEthernet 1/0/1 on Device C. Display the smart link group configuration on Device C.

```

[DeviceC] display smart-link group all
Smart link group 1 information:
Device ID: 000f-e23d-5af0
Preemption mode: ROLE
Preemption delay: 1(s)
Control VLAN: 10
Protected VLAN: Reference Instance 1
Member Role State Flush-count Last-flush-time

GigabitEthernet1/0/1 MASTER ACTIVE 1 17:50:20 2013/02/21
GigabitEthernet1/0/2 SLAVE STANDBY 1 17:45:20 2013/02/21

```

```

Smart link group 2 information:
Device ID: 000f-e23d-5af0
Preemption mode: ROLE
Preemption delay: 1(s)
Control VLAN: 20
Protected VLAN: Reference Instance 2
Member Role State Flush-count Last-flush-time

GigabitEthernet1/0/2 MASTER ACTIVE 0 NA
GigabitEthernet1/0/1 SLAVE STANDBY 0 NA

```

The output shows that:

- The primary link of smart link group 1 becomes active to forward user traffic.
- No link switchover occurs in smart link group 2.

# Display the flush messages received on Device B.

```

[DeviceB] display smart-link flush
Received flush packets : 1

```

```
Receiving interface of the last flush packet : GigabitEthernet1/0/2
Receiving time of the last flush packet : 16:25:21 2013/02/21
Device ID of the last flush packet : 000f-e23d-5af0
Control VLAN of the last flush packet : 10
```

## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```
#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
```

- Device B:

```
#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 smart-link flush enable control-vlan 10 20
#
```

- Device C:

```

#
vlan 1
#
vlan 2 to 20
#
stp region-configuration
 instance 1 vlan 1 to 10
 instance 2 vlan 11 to 20
 active region-configuration
#
smart-link group 1
 preemption mode role
 protected-vlan reference-instance 1
 flush enable control-vlan 10
smart-link group 2
 preemption mode role
 protected-vlan reference-instance 2
 flush enable control-vlan 20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 port smart-link group 1 master
 port smart-link group 2 slave
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 stp disable
 port smart-link group 1 slave
 port smart-link group 2 master
#

```

- **Device D:**

```

#
vlan 1
#
vlan 2 to 20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 smart-link flush enable control-vlan 10 20
#
interface GigabitEthernet1/0/2

```



```
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 to 20
stp disable
smart-link flush enable control-vlan 10 20
#
```

# Monitor Link configuration examples

This chapter provides Monitor Link configuration examples.

Monitor Link works together with Layer 2 topology protocols to adapt the up/down state of a downlink port to the state of an uplink port. This feature enables fast link switchover on a downstream device in response to the uplink state change on its upstream device.

## General configuration restrictions and guidelines

Make sure the port you want to configure as a monitor link group member port is not a member of any aggregation group or service loopback group.

## Example: Configuring Monitor Link

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

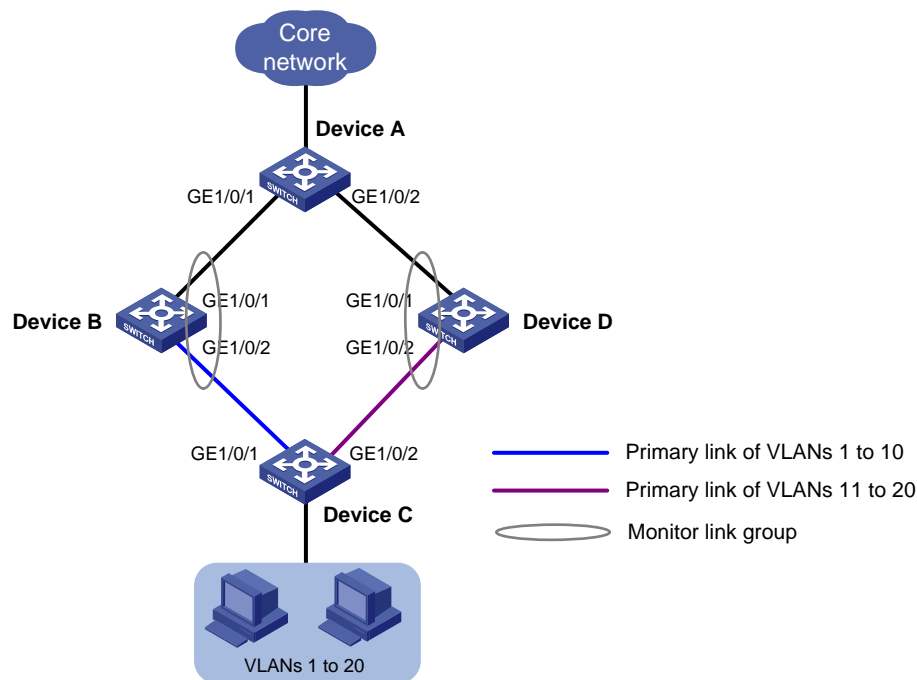
### Network requirements

As shown in [Figure 196](#), traffic of VLANs 1 through 10 and VLANs 11 through 20 on Device C is dually uplinked to Device A through Device B and Device D.

Configure multiple smart link groups on Device C and configure Monitor Link on Device B and Device D to meet the following requirements:

- Traffic of VLANs 1 through 10 is uplinked to Device A by Device B. Traffic of VLANs 11 through 20 is uplinked to Device A by Device D.
- When one forwarding link fails, user traffic is immediately switched to another link to implement dual uplink backup.
- When the link between Device A and Device B (or Device D) fails, Device C can detect the link fault and perform uplink switchover in the smart link group.

Figure 196 Network diagram



## Requirements analysis

For more information about configuring multiple smart link groups, see [“Smart Link configuration examples.”](#)

## Configuration restrictions and guidelines

When you configure Monitor Link, follow these restrictions and guidelines:

- To avoid undesired down/up state changes on the downlink ports, configure uplink ports prior to configuring downlink ports.
- For more information about configuration restrictions and guidelines for configuring multiple smart link groups, see [“Smart Link configuration examples.”](#)

## Configuration procedures

### Configuring Smart Link

For information about smart link group configurations on Device A through Device D, see [“Smart Link configuration examples.”](#)

### Configuring Monitor Link

1. Configure Device B:

```
Create monitor link group 1.
```

```
<DeviceB> system-view
[DeviceB] monitor-link group 1
```

```
Configure GigabitEthernet 1/0/1 as an uplink port and GigabitEthernet 1/0/2 as a downlink
port for monitor link group 1.
```

```
[DeviceB-mtlk-group1] port gigabitethernet 1/0/1 uplink
[DeviceB-mtlk-group1] port gigabitethernet 1/0/2 downlink
[DeviceB-mtlk-group-1] quit
```

## 2. Configure Device D:

```
Create monitor link group 1.
```

```
<DeviceD> system-view
[DeviceD] monitor-link group 1
```

```
Configure GigabitEthernet 1/0/1 as an uplink port and GigabitEthernet 1/0/2 as a downlink
port for monitor link group 1.
```

```
[DeviceD-mtlk-group1] port gigabitethernet 1/0/1 uplink
[DeviceD-mtlk-group1] port gigabitethernet 1/0/2 downlink
[DeviceD-mtlk-group1] quit
```

## Verifying the configuration

```
When GigabitEthernet 1/0/2 on Device A goes down due to a link fault, display information about
monitor link group 1 on Device B.
```

```
[DeviceB] display monitor-link group 1
Monitor link group 1 information:
Group status: UP
Last-up-time: 16:37:20 2013/02/21
Last-down-time: -
Member Role Status

GigabitEthernet1/0/1 UPLINK UP
GigabitEthernet1/0/2 DOWNLINK UP
```

The output shows that both ports in monitor link group 1 are up.

```
Display information about monitor link group 1 on Device D.
```

```
[DeviceD] display monitor-link group 1
Monitor link group 1 information:
Group status: DOWN
Last-up-time: 16:37:27 2013/02/21
Last-down-time: 16:47:19 2013/02/21
Member Role Status

GigabitEthernet1/0/1 UPLINK DOWN
GigabitEthernet1/0/2 DOWNLINK DOWN
```

The output shows that both ports in monitor link group 1 go down because Device D detects that GigabitEthernet 1/0/2 on Device A is down.

# Display smart link group information on Device C.

```
[DeviceC] display smart-link group all
Smart link group 1 information:
Device ID: 000f-e23d-5af0
Preemption mode: ROLE
Preemption delay: 1(s)
Control VLAN: 10
Protected VLAN: Reference Instance 1
Member Role State Flush-count Last-flush-time

GigabitEthernet1/0/1 MASTER ACTIVE 0 NA
GigabitEthernet1/0/2 SLAVE DOWN 0 NA

Smart link group 2 information:
Device ID: 000f-e23d-5af0
Preemption mode: ROLE
Preemption delay: 1(s)
Control VLAN: 20
Protected VLAN: Reference Instance 2
Member Role State Flush-count Last-flush-time

GigabitEthernet1/0/2 MASTER DOWN 0 NA
GigabitEthernet1/0/1 SLAVE ACTIVE 1 16:47:20 2013/02/21
```

The output shows that GigabitEthernet 1/0/2 goes down because Device C detects that the link between Device A and Device D fails and performs a link switchover in smart link group 2. No link switchover occurs in smart link group 1.

## Configuration files

For information about the smart link group configuration files on Device A through Device D, see “[Smart Link configuration examples.](#)”

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device B:

```
#
monitor-link group 1
#
interface GigabitEthernet1/0/1
port link-mode bridge
port monitor-link group 1 uplink
#
interface GigabitEthernet1/0/2
port link-mode bridge
```

```
port monitor-link group 1 downlink
#
```

- Device D:

```
#
monitor-link group 1
#
interface GigabitEthernet1/0/1
port link-mode bridge
port monitor-link group 1 uplink
#
interface GigabitEthernet1/0/2
port link-mode bridge
port monitor-link group 1 downlink
#
```

# Software upgrade configuration examples

This chapter provides examples for each task in the software 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

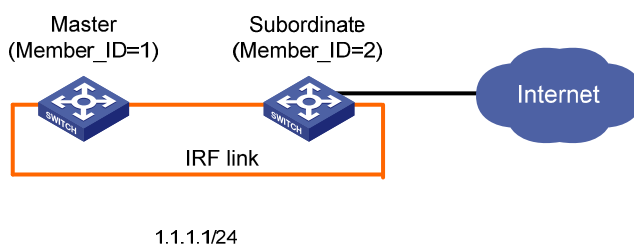
| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

### Network requirements

As shown in [Figure 197](#):

- Verify that the member switches in the IRF fabric have a sufficient storage space for software images.
- Backup the configuration files.

**Figure 197 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- 20070016 Apr 26 2012 12:45:21 bootfile-e1109.bin
1 -rw- 151 Apr 26 2012 12:12:54 system.xml
2 -rw- 2019 Apr 26 2012 12:12:56 startup.cfg
3 -rw- 21527220 Apr 26 2012 13:06:45 bootfile-e1108.bin
4 -rw- 21527956 Apr 26 2012 12:38:22 bootfile-e1107.bin
5 -rw- 21280832 Apr 26 2012 13:09:13 bootfile-e1106.bin
6 -rw- 20840600 Apr 26 2012 12:07:00 bootfile-e1105.bin
7 -rw- 20594888 Apr 26 2012 12:09:59 bootfile-e1104.bin

```

515712 KB total (18604 KB free)

# Display files and subdirectories in the root directory of the flash memory on the subordinate switch.

```

<Sysname> cd slot2#flash:/
<Sysname> dir
Directory of slot2#flash:/

```

```

0 -rw- 21280832 Apr 26 2012 13:09:30 bootfile-e1109.bin
1 -rw- 20840600 Apr 26 2012 12:09:02 bootfile-e1106.bin
2 -rw- 20780880 Apr 24 2013 16:58:21 bootfile-e1105.bin
3 -rw- 21604876 Apr 26 2012 14:04:36 bootfile-e1108.bin
4 -rw- 151 Aug 31 2013 11:47:59 system.xml
5 -rw- 2508 Apr 26 2012 13:01:15 startup.cfg
6 -rw- 21527220 Apr 26 2012 18:06:53 bootfile-e1107.bin
7 -rw- 21527956 Apr 26 2012 12:22:15 bootfile-e1103.bin
8 -rw- 20594888 Mar 25 2013 16:31:07 bootfile-e1104.bin

```

515712 KB total (167528 KB free)

# Delete unused files to ensure a sufficient storage space. In this example, delete **bootfile-e1104.bin** from all IRF member switches.

```

<Sysname>delete /unreserved bootfile-e1104.bin
The contents cannot be restored!!! Delete flash:/bootfile-e1104.bin?[Y/N]:y
Deleting a file permanently will take a long time. Please wait...

```

%Delete file flash:/bootfile-e1104.bin...Done.

```

<Sysname> delete /unreserved slot2#flash:/bootfile-e1104.bin
Delete slot2#flash:/bootfile-e1104.bin?[Y/N]:y

```

%Delete file slot2#flash:/bootfile-e1104.bin...Done.

# Rename the configuration file **startup.cfg** to **startup\_old.cfg** on the master switch.

```

<Sysname>rename startup.cfg startup_old.cfg
Rename flash:/startup.cfg to flash:/startup_old.cfg?[Y/N]:y

```

%Renamed file flash:/startup.cfg to flash:/startup\_old.cfg.

# Create the **backup** directory in the root directory of the flash memory on the master switch.

```

<Sysname>mkdir backup

```



```

%Created dir flash:/backup.

Copy startup_old.cfg to the backup directory on the master switch.
<Sysname> copy startup_old.cfg backup
Copy flash:/startup_old.cfg to flash:/backup/startup_old.cfg?[Y/N]:y
.
%Copy file flash:/startup_old.cfg to flash:/backup/startup_old.cfg...Done.

Rename startup.cfg on the subordinate switch to startup_old.cfg.
<Sysname>rename slot2#flash:/startup.cfg slot2#flash:/startup_old.cfg
Rename slot2#flash:/startup.cfg to slot2#flash:/startup_old.cfg?[Y/N]:y

%Renamed file slot2#flash:/startup.cfg to slot2#flash:/startup_old.cfg.

Create the backup directory in the root directory of the flash memory on the subordinate switch.
<Sysname>mkdir slot2#flash:/backup

%Created dir slot2#flash:/backup.

Copy startup_old.cfg to the backup directory on the subordinate switch.
<Sysname> copy slot2#flash:/startup_old.cfg slot2#flash:/backup
Copy slot2#flash:/startup_old.cfg to slot2#flash:/backup/startup_old.cfg?[Y/N]:y
.
%Copy file slot2#flash:/startup_old.cfg to slot2#flash:/backup/startup_old.cfg...Done.

```

## Verifying the configuration

# Execute the **dir** command and **more** command to verify the file operations.

The output shows that:

- The **bootfile-e1104.bin** file and the **startup.cfg** file do not exist in the root directory of the flash memory on the master switch. The **startup\_old.cfg** file and the **backup** directory exist in the root directory of the flash memory on the master switch.
- The **bootfile-e1104.bin** file and the **startup.cfg** file do not exist in the root directory of the flash memory on the subordinate switch. The **startup\_old.cfg** file and the **backup** directory exist in the root directory of the flash memory on the subordinate switch.

## Configuration files

The system does not save file operations to a configuration file.

# Example: Downloading software from an FTP server

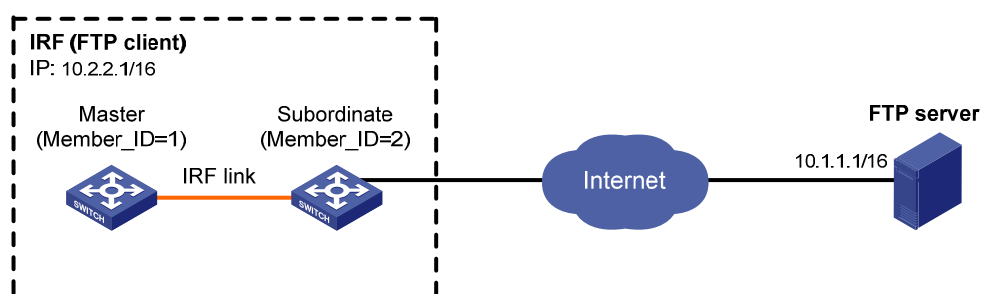
## Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in [Figure 198](#), use the IRF fabric as an FTP client to download software images from an FTP server.

**Figure 198 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 and the FTP user account has been configured on the FTP server.

1. Configure the master switch.

```
Use the user name and password to log in to the FTP server.
```

```
<Sysname> ftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 FTP service ready.
User(10.1.1.1:(none)):abc
```

```

331 Password required for abc.
Password:
230 User logged in.
Set the file transfer mode to binary.
[ftp] binary
200 Type set to I.
Download the Boot ROM upgrade image (bootrom.btm) from the FTP server to the flash memory
of the master switch.
[ftp]get bootrom.btm
227 Entering Passive Mode (10,1,1,1,4,8).
125 BINARY mode data connection already open, transfer starting for /bootrom.btm.
226 Transfer complete.
FTP: 338736 byte(s) received in 1.488 second(s), 227.00K byte(s)/sec.
Download the system software image (bootfile.bin) from the FTP server to the flash memory of the
master switch.
[ftp] get bootfile.bin
227 Entering Passive Mode (10,1,1,1,4,9).
125 BINARY mode data connection already open, transfer starting for bootfile.bin.
226 Transfer complete.
FTP: 9875040 byte(s) received in 126.253 second(s) 78.00K byte(s)/sec.
Download the configuration file startup.cfg from the FTP server to the flash memory of the master
switch.
[ftp]get startup.cfg
227 Entering Passive Mode (10,1,1,1,4,10).
125 BINARY mode data connection already open, transfer starting for /startup.cfg.
226 Transfer complete.
FTP: 2478 byte(s) received in 0.136 second(s), 18.00K byte(s)/sec.
[ftp] bye

```

2. Configure the subordinate switch in the same way you configure the master switch.

## Verifying the configuration

```

Verify that the files have been downloaded.
<Sysname>dir
Directory of flash:/
 0 -rw- 9875040 Apr 26 2000 13:08:36 bootfile.bin
 1 -rw- 338736 Apr 26 2000 13:06:57 bootrom.btm
 2 -rw- 2478 Apr 26 2000 12:45:01 startup.cfg
31496 KB total (17708 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 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in [Figure 199](#), the IRF fabric is an FTP server. Use an FTP client to upload software images to the IRF fabric.

**Figure 199 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:

# Enable the FTP server function.

```
<Sysname> system-view
```

```
[Sysname] ftp server enable
```

# Add a local user account, set the username to **abc**, and set the password to **pwd**.

```
[Sysname] local-user abc
```

```
[Sysname-luser-abc] password simple pwd
```

# Set the service type to **ftp**.

```
[Sysname-luser-abc] service-type ftp
```

# Set the user privilege level to **3**.

```
[Sysname-luser-abc] authorization-attribute level 3
[Sysname-luser-abc] quit
```

## 2. Transfer upgrade files from the FTP client to the IRF fabric:

# Use the username and the password 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 set to I.
```

# Upload the Boot ROM image **bootrom.btm** to the master switch.

```
ftp> put bootrom.btm
200 Port command okay.
150 Opening BINARY mode data connection for /bootrom.btm.
226 Transfer complete.
ftp: 463364 bytes sent in 2.23 seconds (207.32 Kbyte/s).
```

# Upload the system software image **bootfile.bin** to the master switch.

```
ftp> put bootfile.bin
200 Port command okay.
150 Opening BINARY mode data connection for /bootfile.bin.
226 Transfer complete.
ftp: 9875040 bytes sent in 126.253 Seconds (87.32 Kbyte/s).
```

# Upload the configuration file **startup.cfg** to the master switch.

```
ftp> put startup.cfg
200 Port command okay.
150 Opening BINARY mode data connection for /startup.cfg.
226 Transfer complete.
ftp: 737556 bytes sent in 7.02 Seconds (390.24 Kbyte/s).
```

## Verifying the configuration

# Verify that the files have been uploaded to the IRF fabric.

```
<Sysname>dir
Directory of flash:/
 0 -rw- 9875040 Apr 26 2000 13:08:36 bootfile.bin
 1 -rw- 338736 Apr 26 2000 13:06:57 bootrom.btm
 2 -rw- 2478 Apr 26 2000 12:45:01 startup.cfg
31496 KB total (17708 KB free)
```

## Configuration files

```
#
ftp server enable
#
local-user abc
password simple pwd
authorization-attribute level 3
service-type ftp
#
```

## Example: Downloading software from a TFTP server

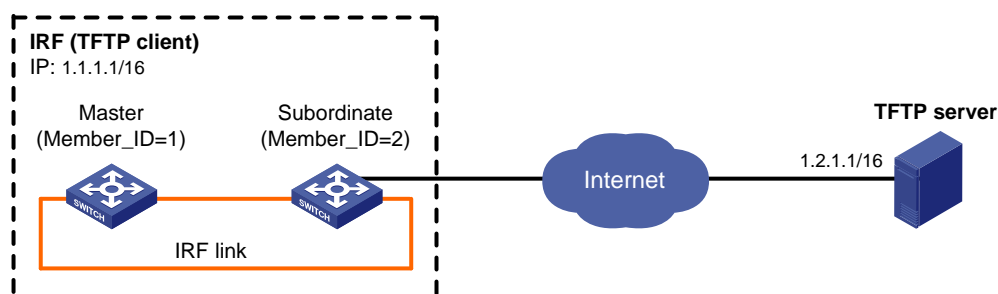
### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in [Figure 200](#), use the IRF fabric as a TFTP client to download software images from a TFTP server.

**Figure 200 Network diagram**



## Configuration procedures

This example assumes that the TFTP server and the IRF fabric can ping each other.

1. Configure the master switch.
  - # Download the Boot ROM image **bootrom.btm** to the flash memory of the master switch.

```

<Sysname> tftp 1.2.1.1 get bootrom.btm
 File will be transferred in binary mode
 Downloading file from remote TFTP server, please wait...\
 TFTP: 463364 bytes received in 6 second(s)
 File downloaded successfully.

Download the system software image bootfile.bin to the flash memory of the master switch.

<Sysname> tftp 1.2.1.1 get bootfile.bin
 File will be transferred in binary mode
 Downloading file from remote TFTP server, please wait...\
 TFTP: 9875040 bytes received in 126 second(s)
 File downloaded successfully.

Download the configuration file startup.cfg to the flash memory of the master switch.

<Sysname> tftp 1.2.1.1 get startup.cfg
 File will be transferred in binary mode
 Downloading file from remote TFTP server, please wait...\
 TFTP: 863356 bytes received in 8 second(s)
 File downloaded successfully.

```

2. Configure the subordinate switch in the same way you configure the master switch.

## Verifying the configuration

```

Verify that the files have been downloaded.

<Sysname>dir
Directory of flash:/
 0 -rw- 9875040 Apr 26 2000 13:08:36 bootfile.bin
 1 -rw- 338736 Apr 26 2000 13:06:57 bootrom.btm
 2 -rw- 2478 Apr 26 2000 12:45:01 startup.cfg
31496 KB total (17708 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

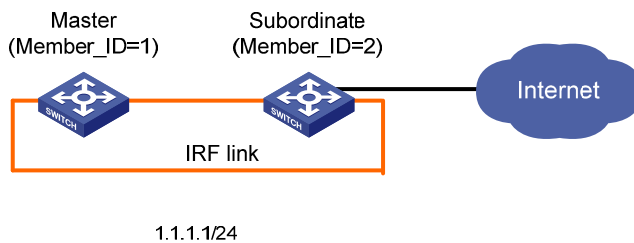
| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in [Figure 201](#), the startup software and configuration files have been stored in the flash memory of the master switch.

Use the files to upgrade the IRF fabric.

**Figure 201 Network diagram**



## Configuration restrictions and guidelines

All member switches must use the same software image version.

## Configuration procedures

# Copy the upgrade software image from the master switch to the root directory of the flash on the subordinate switch.

```
<Sysname> copy bootfile-e1110.bin slot2#flash:/
Copy flash:/bootfile-e1110.bin to slot2#flash:/bootfile-e1110.bin?[Y/N]:y
```

```
%Copy file flash:/bootfile-e1110.bin to slot2#flash:/bootfile-e1110.bin...Done.
```

# Upgrade the Boot ROM of the master switch.

```
<Sysname>bootrom update file bootfile-e1110.bin slot 1
This command will update bootrom file on the specified board(s), Continue? [Y/N]:y
```

```
Now updating bootrom, please wait...
```

# Upgrade the Boot ROM of the subordinate switch.

```
<Sysname>bootrom update file bootfile-e1110.bin slot 2
This command will update bootrom file on the specified board(s), Continue? [Y/N]:y
```

```
Now updating bootrom, please wait...
```

# Specify **bootfile-e1110.bin** as the main startup image file and **bootfile-e1109.bin** as the backup startup image file for the master switch.

```
<Sysname>boot-loader file bootfile-e1110.bin slot 1 main
This command will set the boot file of the specified board. Continue? [Y/N]:y
```



```

 The specified file will be used as the main boot file at the next reboot on slot 1!
<Sysname>boot-loader file bootfile-e1109.bin slot 1 backup
 This command will set the boot file. Continue? [Y/N]:y
 The specified file will be used as the backup boot file at the next reboot on slot 1!
Specify bootfile-e1110.bin as the main startup image file and bootfile-e1109.bin as the backup startup
image file for the subordinate switch.
<Sysname>boot-loader file bootfile-e1110.bin slot 2 main
 This command will set the boot file of the specified board. Continue? [Y/N]:y
 The specified file will be used as the main boot file at the next reboot on slot 2!
<Sysname>boot-loader file bootfile.bin slot 2 backup
 This command will set the boot file. Continue? [Y/N]:y
 The specified file will be used as the backup boot file at the next reboot on slot 2!
Change the file name of startup.cfg to startup_new.cfg in the flash memory of the master switch.
<Sysname>rename startup.cfg startup_new.cfg
Rename flash:/startup.cfg to flash:/startup_new.cfg?[Y/N]:y

%Renamed file flash:/startup.cfg to flash:/startup_new.cfg.
Specify startup_new.cfg as the main next-startup configuration file and startup_old.cfg as the backup
next-startup configuration file.
<Sysname>startup saved-configuration startup_new.cfg main
Please wait ...
Setting the master board ...
... Done!

<Sysname>startup saved-configuration startup_old.cfg backup
Please wait ...
Setting the master board ...
... Done!
Reboot the IRF fabric.
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait.
.....DONE!
 This command will reboot the switch. Current configuration may be lost in next startup
if you continue. Continue? [Y/N]:y

```

## Verifying the configuration

- # Use the **display version** command to verify that the software has been upgraded.
- # Use the **display startup** command to verify that the configuration file settings are correct.

## 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 any of the following functions on a port:

- Service loopback
- Rapid Ring Protection Protocol (RRPP)
- Smart Link
- BPDU tunneling for STP

## Example: Configuring MSTP

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

### Network requirements

As shown in [Figure 202](#):

- 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 203](#).

Figure 202 Network diagram

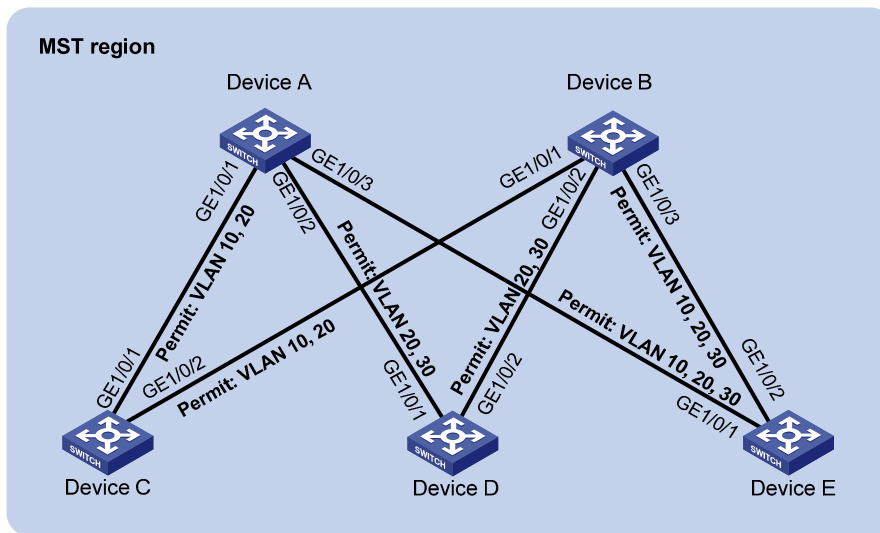
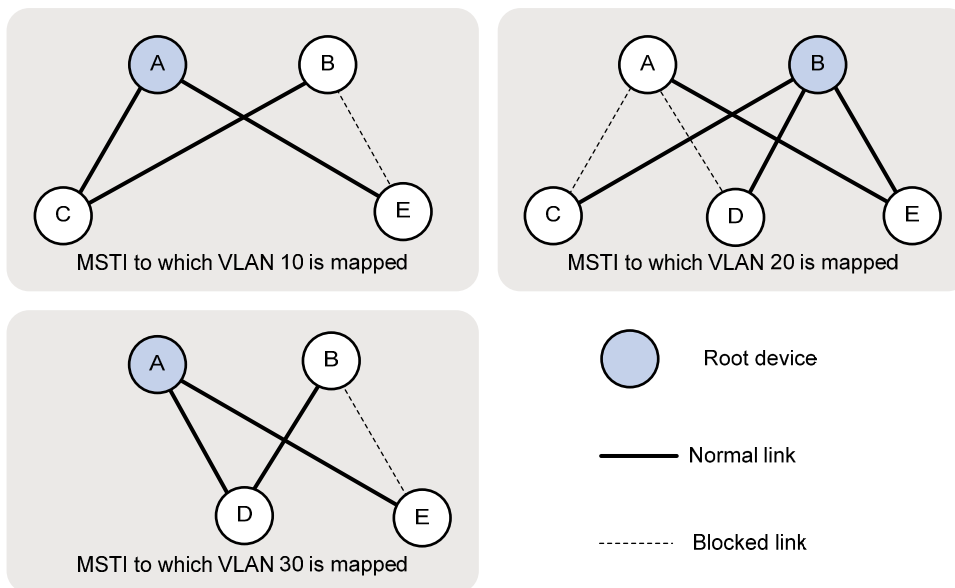


Figure 203 MSTI to which each VLAN is mapped



## Requirements analysis

To forward packets from different VLANs along different physical links, you can 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.

In this example, the path cost calculation standard is **legacy** for all devices, and the default path cost of each port is 20.

# Configuration restrictions and guidelines

When you configure MSTP, follow these restrictions and guidelines:

- Two or more spanning tree devices belong to the same MST region only if both of the following are true:
  - The devices are configured to have the same format selector (0 by default, not configurable), MST region name, MST region revision level, and VLAN-to-instance mappings in the MST region.
  - The devices are connected through physical links.
- 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.
- You can use the **stp mcheck** command in system view or port view.
  - Using the **stp mcheck** command in system view takes effect on all ports.
  - Using the **stp mcheck** command in port view takes effect on only the port.

## Configuration procedures

### Configuring VLANs and ports

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 GigabitEthernet 1/0/1 as a trunk port.
```

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

```
Remove GigabitEthernet 1/0/1 from VLAN 1.
```

```
[DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
Assign GigabitEthernet 1/0/1 to VLANs 10 and 20.
```

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 10 20
```

```
Enable the spanning tree protocol on GigabitEthernet 1/0/1. By default, the spanning tree protocol is enabled on a port.
```

```
[DeviceA-GigabitEthernet1/0/1] stp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

```
Configure GigabitEthernet 1/0/2 as a trunk port.
```

```
[DeviceA] interface gigabitethernet 1/0/2
```

```

[DeviceA-GigabitEthernet1/0/2] port link-type trunk
Remove GigabitEthernet 1/0/2 from VLAN 1.
[DeviceA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
Assign GigabitEthernet 1/0/2 to VLANs 20 and 30.
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 20 30
Enable the spanning tree protocol on GigabitEthernet 1/0/2. By default, the spanning tree
protocol is enabled on a port.
[DeviceA-GigabitEthernet1/0/2] stp enable
[DeviceA-GigabitEthernet1/0/2] quit
Configure GigabitEthernet 1/0/3 as a trunk port.
[DeviceA] interface gigabitethernet 1/0/3
Remove GigabitEthernet 1/0/3 from VLAN 1.
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] undo port trunk permit vlan 1
Assign GigabitEthernet 1/0/3 to VLANs 10, 20, and 30.
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 10 20 30
Enable the spanning tree protocol on GigabitEthernet 1/0/3. By default, the spanning tree
protocol is enabled on a port.
[DeviceA-GigabitEthernet1/0/3] stp enable
[DeviceA-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 enable
```
8. Perform an mCheck operation globally to make sure all ports of Device A are operating in MSTP mode.
 

```
[DeviceA] stp 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 enable`
8. Perform an mCheck operation globally to make sure all ports of Device B are operating in MSTP mode.  
`[DeviceB] stp 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.  
`[DeviceC-mst-region] check region-configuration`
3. Activate the MST region configuration.  
`[DeviceC-mst-region] active region-configuration`  
`[DeviceC-mst-region] quit`
4. Set the path cost of port GigabitEthernet 1/0/1 in MSTI 1 to 15.  
`[DeviceC] interface gigabitethernet 1/0/1`  
`[DeviceC-GigabitEthernet1/0/1] stp instance 1 cost 15`  
`[DeviceC-GigabitEthernet1/0/1] quit`
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 enable`
7. Perform an mCheck operation globally to make sure all ports of Device B are operating in MSTP mode.  
`[DeviceC] stp 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 configuration.

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```
4. Set the path cost of port GigabitEthernet 1/0/1 in MSTI 2 to 15.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] stp instance 2 cost 15
[DeviceD-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 enable
```
7. Perform an mCheck operation globally to make sure all ports of Device B are operating in MSTP mode.

```
[DeviceD] stp 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 GigabitEthernet 1/0/2 of Device E in MSTI 0 to 15.


```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] stp instance 0 cost 15
[DeviceE-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 enable
```
 7. Perform an mCheck operation globally to make sure all ports of Device B are operating in MSTP mode.


```
[DeviceE] stp mcheck
```

Verifying the configuration

When the network is stable, use the **display stp brief** command to display brief spanning tree information on each device.

Display brief spanning tree information on Device A.

```
[DeviceA] display stp brief
```

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/1	ALTE	DISCARDING	NONE
0	GigabitEthernet1/0/2	ALTE	DISCARDING	NONE
0	GigabitEthernet1/0/3	ROOT	FORWARDING	NONE
1	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
1	GigabitEthernet1/0/3	DESI	FORWARDING	NONE
2	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
2	GigabitEthernet1/0/3	DESI	FORWARDING	NONE

Display brief spanning tree information on Device B.

```
[DeviceB] display stp brief
```

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/3	DESI	FORWARDING	NONE
1	GigabitEthernet1/0/1	ROOT	FORWARDING	NONE
1	GigabitEthernet1/0/3	ALTE	DISCARDING	NONE
2	GigabitEthernet1/0/2	ROOT	FORWARDING	NONE
2	GigabitEthernet1/0/3	ALTE	DISCARDING	NONE

Display brief spanning tree information on Device C.

```
[DeviceC] display stp brief
```

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/2	ROOT	FORWARDING	NONE
1	GigabitEthernet1/0/1	ROOT	FORWARDING	NONE
1	GigabitEthernet1/0/2	DESI	FORWARDING	NONE

Display brief spanning tree information on Device D.

```
[DeviceD] display stp brief
```

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/2	ROOT	FORWARDING	NONE
2	GigabitEthernet1/0/1	ROOT	FORWARDING	NONE
2	GigabitEthernet1/0/2	DESI	FORWARDING	NONE

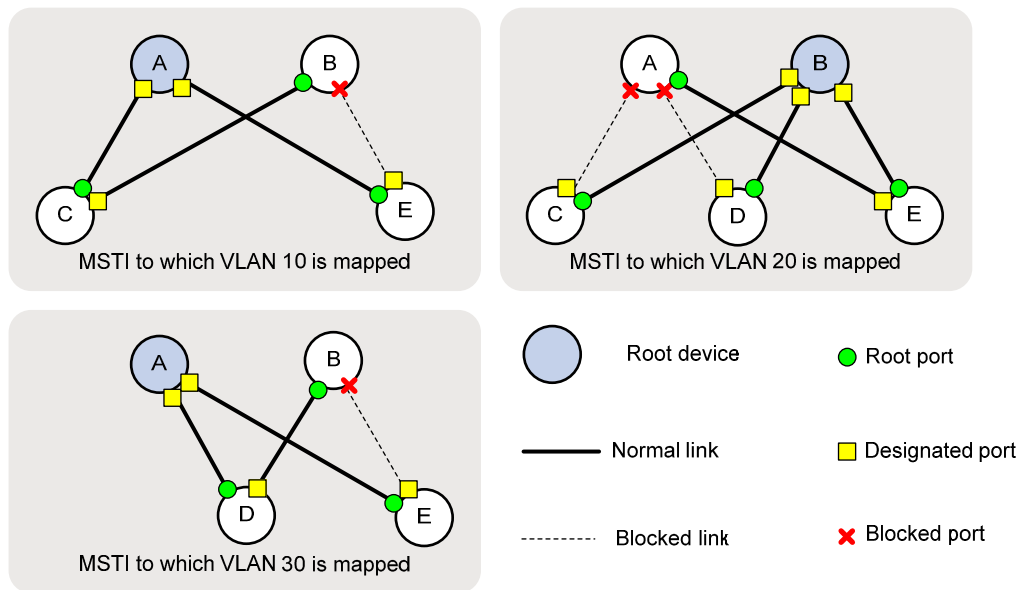
Display brief spanning tree information on Device E.

```
[DeviceE] display stp brief
```

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/2	ROOT	FORWARDING	NONE
1	GigabitEthernet1/0/1	ROOT	FORWARDING	NONE
1	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
2	GigabitEthernet1/0/1	ROOT	FORWARDING	NONE
2	GigabitEthernet1/0/2	DESI	FORWARDING	NONE

Based on the output, you can draw the MSTI to which each VLAN is mapped, as shown in [Figure 204](#). The figure shows that the configuration meets the network requirements.

Figure 204 MSTI to which each VLAN is mapped



Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:


```
#
vlan 10
#
```

```

vlan 20
#
vlan 30
#
stp region-configuration
  region-name example
  instance 1 vlan 10
  instance 2 vlan 30
  active region-configuration
#
stp instance 0 root secondary
stp instance 1 root primary
stp instance 2 root primary
stp enable
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 10 20
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 20 30
#
interface GigabitEthernet1/0/3
  port link-mode bridge
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 10 20 30
#

```

- **Device B:**

```

#
vlan 10
#
vlan 20
#
vlan 30
#
stp region-configuration
  region-name example
  instance 1 vlan 10
  instance 2 vlan 30
  active region-configuration
#
stp instance 0 root primary

```

```

stp instance 1 root secondary
stp instance 2 root secondary
stp enable
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 20 30
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30
#

```

- **Device C:**

```

#
vlan 10
#
vlan 20
#
stp region-configuration
region-name example
instance 1 vlan 10
instance 2 vlan 30
active region-configuration
#
stp enable
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20
stp instance 1 cost 15
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20

```

- ```

#

```
- **Device D:**

```

#
vlan 20
#
vlan 30
#
stp region-configuration
 region-name example
 instance 1 vlan 10
 instance 2 vlan 30
 active region-configuration
#
stp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
 stp instance 2 cost 15
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
#

```
  - **Device E:**

```

#
vlan 10
#
vlan 20
#
vlan 30
#
stp region-configuration
 region-name example
 instance 1 vlan 10
 instance 2 vlan 30
 active region-configuration
#
stp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1

```

```
port trunk permit vlan 10 20 30
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20 30
stp instance 0 cost 15
#
```

## Example: Configuring RSTP

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

### Network requirements

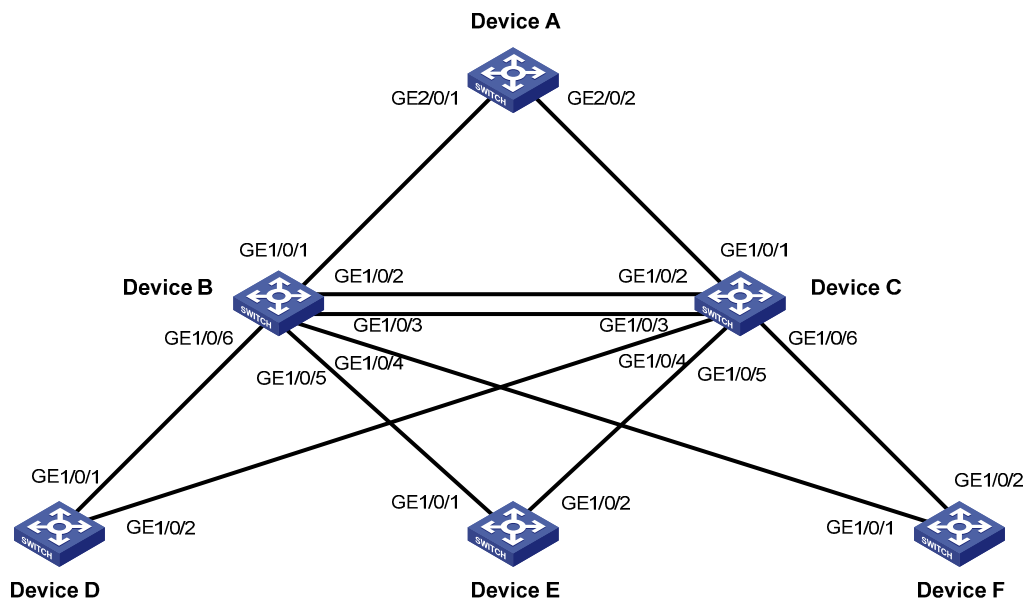
As shown in [Figure 205](#), the LAN has multiple layers:

- 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.
- In this example, all ports of these devices have the same path cost.

Configure RSTP to meet the following requirements:

- Device A is the root bridge. Root guard is enabled on the device to protect the device against configuration errors and malicious attacks.
- Device C backs up Device B. When Device B fails, Device C takes over to forward data traffic.
- The ports of Device D, Device E, and Device F that directly connect to users are configured as edge ports. BPDU guard is enabled on these ports.
- The network is stable and protected against forged TC-BPDUs.

Figure 205 Network diagram



NOTE:

- Device A is typically a high-end or mid-range switch, for example, an HP 10500 switch.
- Device B and Device C are typically the HP 5800 or 5500 switches of the low-end switches.
- Device D, Device E, and Device F are typically the HP 3600 v2 switches of the low-end switches.

## 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 section describes 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 GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] stp root-protection
[DeviceA-GigabitEthernet2/0/1] quit
[DeviceA] interface GigabitEthernet 2/0/2
[DeviceA-GigabitEthernet2/0/2] stp root-protection
[DeviceA-GigabitEthernet2/0/2] quit

Enable TC-BPDU guard on Device A. TC-BPDU guard is enabled by default.
[DeviceA] stp tc-protection enable

Enable RSTP globally.
[DeviceA] stp enable

Perform an mCheck operation globally to make sure all ports of the device are operating in RSTP mode.
[DeviceA] stp mcheck

Disable STP on the ports that do not participate in the RSTP calculation. This example uses
GigabitEthernet 2/0/4.
[DeviceA] interface GigabitEthernet 2/0/4
[DeviceA-GigabitEthernet2/0/4] undo stp enable
[DeviceA-GigabitEthernet2/0/4] quit
```

## Configuring Device B

```
Set the spanning tree mode to RSTP.
<DeviceB> system-view
[DeviceB] stp mode rstp

Set the device priority to 4096 for Device B.
[DeviceB] stp priority 4096

Enable root guard on each designated port.
[DeviceB] interface GigabitEthernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] stp root-protection
[DeviceB-GigabitEthernet1/0/4] quit
[DeviceB] interface GigabitEthernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] stp root-protection
[DeviceB-GigabitEthernet1/0/5] quit
```



```

[DeviceB] interface GigabitEthernet 1/0/6
[DeviceB-GigabitEthernet1/0/6] stp root-protection
[DeviceB-GigabitEthernet1/0/6] quit

Use the default settings for the spanning tree timers and other port parameters.

Enable RSTP globally.
[DeviceB] stp enable

Perform an mCheck operation globally to make sure all ports of the device are operating in RSTP mode.
[DeviceB] stp mcheck

Disable STP on the ports that do not participate in the RSTP calculation. This example uses
GigabitEthernet 1/0/8.
[DeviceB] interface GigabitEthernet 1/0/8
[DeviceB-GigabitEthernet1/0/8] undo stp enable
[DeviceB-GigabitEthernet1/0/8] quit

```

## Configuring Device C

```

Set the spanning tree mode to RSTP.
<DeviceC> system-view
[DeviceC] stp mode rstp

Set the device priority to 8192 for Device C, so that Device C serves as the backup of Device B.
[DeviceC] stp priority 8192

Enable root guard on each designated port.
[DeviceC] interface GigabitEthernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] stp root-protection
[DeviceC-GigabitEthernet1/0/4] quit
[DeviceC] interface GigabitEthernet 1/0/5
[DeviceC-GigabitEthernet1/0/5] stp root-protection
[DeviceC-GigabitEthernet1/0/5] quit
[DeviceC] interface GigabitEthernet 1/0/6
[DeviceC-GigabitEthernet1/0/6] stp root-protection
[DeviceC-GigabitEthernet1/0/6] quit

Use the default settings for the spanning tree timers and other port parameters.

Enable RSTP globally.
[DeviceC] stp enable

Perform an mCheck operation globally to make sure all ports of the device are operating in RSTP mode.
[DeviceC] stp mcheck

Disable STP on the ports that do not participate in the RSTP calculation. This example uses
GigabitEthernet 1/0/8.
[DeviceC] interface GigabitEthernet 1/0/8
[DeviceC-GigabitEthernet1/0/8] undo stp enable
[DeviceC-GigabitEthernet1/0/8] quit

```

## Configuring Device D

```

Set the spanning tree mode to RSTP.

```

```
<DeviceD> system-view
[DeviceD] stp mode rstp
```

# Configure the ports directly connecting to users as edge ports, and enable BPDU guard on them. (This example uses GigabitEthernet 1/0/4.)

```
[DeviceD] interface GigabitEthernet 1/0/4
[DeviceD-GigabitEthernet1/0/4] stp edged-port enable
[DeviceD-GigabitEthernet1/0/4] quit
[DeviceD] stp bpdu-protection
```

# Use the default settings for the spanning tree timers and other port parameters.

# Enable RSTP globally.

```
[DeviceD] stp enable
```

# Perform an mCheck operation globally to make sure all ports of the device are operating in RSTP mode.

```
[DeviceD] stp mcheck
```

# Disable STP on the ports that do not participate in the RSTP calculation. This examples uses GigabitEthernet 1/0/3.

```
[DeviceD] interface GigabitEthernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] undo stp enable
[DeviceD-GigabitEthernet1/0/3] quit
```

## Configuring Device E and Device F

Configure Device E and Device F in the same way Device D is configured.

## Verifying the configuration

When the network is stable, use the **display stp brief** command to display brief spanning tree information on each device.

# Display brief spanning tree information on Device A.

```
[DeviceA] display stp brief
```

| MSTID | Port                 | Role | STP State  | Protection |
|-------|----------------------|------|------------|------------|
| 0     | GigabitEthernet1/0/1 | DESI | FORWARDING | ROOT       |
| 0     | GigabitEthernet1/0/2 | DESI | FORWARDING | ROOT       |

# Display brief spanning tree information on Device B.

```
[DeviceB] display stp brief
```

| MSTID | Port                 | Role | STP State  | Protection |
|-------|----------------------|------|------------|------------|
| 0     | GigabitEthernet1/0/1 | ROOT | FORWARDING | NONE       |
| 0     | GigabitEthernet1/0/2 | DESI | FORWARDING | NONE       |
| 0     | GigabitEthernet1/0/3 | DESI | FORWARDING | NONE       |
| 0     | GigabitEthernet1/0/4 | DESI | FORWARDING | ROOT       |
| 0     | GigabitEthernet1/0/5 | DESI | FORWARDING | ROOT       |
| 0     | GigabitEthernet1/0/6 | DESI | FORWARDING | ROOT       |

# Display brief spanning tree information on Device C.

```
[DeviceC] display stp brief
```

| MSTID | Port | Role | STP State | Protection |
|-------|------|------|-----------|------------|
|-------|------|------|-----------|------------|

```

0 GigabitEthernet1/0/1 ROOT FORWARDING NONE
0 GigabitEthernet1/0/2 ALTE DISCARDING NONE
0 GigabitEthernet1/0/3 ALTE DISCARDING NONE
0 GigabitEthernet1/0/4 DESI FORWARDING ROOT
0 GigabitEthernet1/0/5 DESI FORWARDING ROOT
0 GigabitEthernet1/0/6 DESI FORWARDING ROOT

```

# Display brief spanning tree information on Device D.

```

[DeviceD] display stp brief
MSTID Port Role STP State Protection
0 GigabitEthernet1/0/1 ROOT FORWARDING NONE
0 GigabitEthernet1/0/2 ALTE DISCARDING NONE
0 GigabitEthernet1/0/4 DESI FORWARDING NONE

```

# Display brief spanning tree information on Device E.

```

[DeviceE] display stp brief
MSTID Port Role STP State Protection
0 GigabitEthernet1/0/1 ROOT FORWARDING NONE
0 GigabitEthernet1/0/2 ALTE DISCARDING NONE
0 GigabitEthernet1/0/4 DESI FORWARDING NONE

```

# Display brief spanning tree information on Device F.

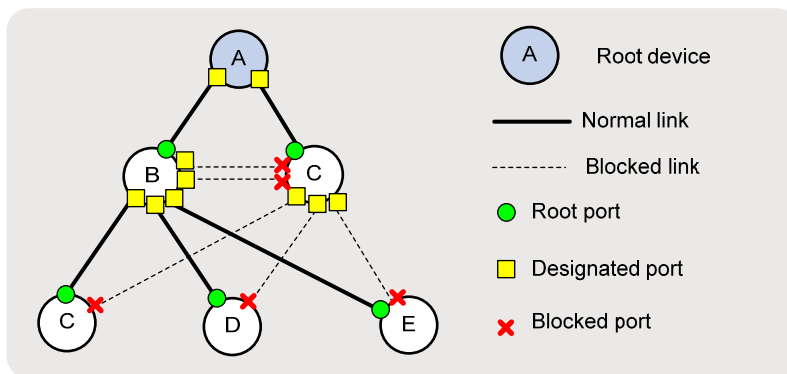
```

[DeviceF] display stp brief
MSTID Port Role STP State Protection
0 GigabitEthernet1/0/1 ROOT FORWARDING NONE
0 GigabitEthernet1/0/2 ALTE DISCARDING NONE
0 GigabitEthernet1/0/4 DESI FORWARDING NONE

```

Based on the output, you can draw the topology when the network is stable, as shown in [Figure 206](#).

**Figure 206 Network topology**



## Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```

#
 stp mode rstp
 stp instance 0 root primary
 stp enable
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet2/0/2
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet2/0/4
 port link-mode bridge
 stp disable
#

```

- **Device B:**

```

#
 stp mode rstp
 stp instance 0 priority 4096
 stp enable
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet1/0/8
 port link-mode bridge
 stp disable
#

```

- **Device C:**

```

#
 stp mode rstp
 stp instance 0 priority 8192
 stp enable
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 stp root-protection

```

```

#
interface GigabitEthernet1/0/5
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet1/0/8
 port link-mode bridge
 stp disable

```

- Device D:

```

#
 stp mode rstp
 stp bpdu-protection
 stp enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 stp disable
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 stp edged-port enable
#

```

## Example: Configuring interoperability with a third-party device that uses a private key to calculate the configuration digest

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

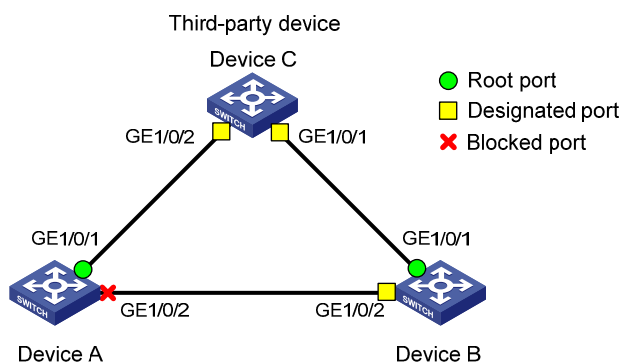
The configuration digest is 16 bytes and is the result calculated by using the HMAC-MD5 algorithm based on VLAN-to-instance mappings. Because spanning tree implementations vary with vendors, the configuration digests calculated through private keys are different. As a result, devices from different vendors in the same MST region cannot communicate with each other.

As shown in [Figure 207](#):

- 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 207 Network diagram**



## Configuration restrictions and guidelines

When you configure digest snooping, follow these restrictions and guidelines:

- HP recommends that you enable digest snooping first and then the spanning tree protocol. To avoid traffic interruption, do not configure digest snooping when the network is already working 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 enable
```

6. Perform an mCheck operation globally to make sure all ports of Device A are operating in MSTP mode.

```
[DeviceA] stp 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 Device A

```
Enable digest snooping on port GigabitEthernet 1/0/1.
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceA-GigabitEthernet1/0/1] quit

Enable digest snooping globally.
[DeviceA] stp config-digest-snooping
```

## Configuring digest snooping Device B

```
Enable digest snooping on port GigabitEthernet 1/0/1.
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceB-GigabitEthernet1/0/1] quit

Enable digest snooping globally.
[DeviceB] stp config-digest-snooping
```

## Verifying the configuration

# Display brief spanning tree information on Device A.

```
[DeviceA] display stp brief
```

| MSTID | Port                 | Role | STP State  | Protection |
|-------|----------------------|------|------------|------------|
| 0     | GigabitEthernet1/0/1 | ROOT | FORWARDING | NONE       |
| 0     | GigabitEthernet1/0/2 | ALTE | DISCARDING | NONE       |

# Display brief spanning tree information on Device B.

```
[DeviceB] display stp brief
```

| MSTID | Port                 | Role | STP State  | Protection |
|-------|----------------------|------|------------|------------|
| 0     | GigabitEthernet1/0/1 | ROOT | FORWARDING | NONE       |
| 0     | GigabitEthernet1/0/2 | DESI | FORWARDING | NONE       |

# Display the root bridge of HP devices, for example, Device A.

```
<DeviceA> display stp root
```

| MSTID | Root Bridge ID   | ExtPathCost | IntPathCost | Root Port            |
|-------|------------------|-------------|-------------|----------------------|
| 0     | 0.00e0-fc0e-6554 | 20          | 0           | 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

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:



```

#
stp region-configuration
 region-name example
 active region-configuration
#
 stp enable
#
 stp config-digest-snooping
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 stp config-digest-snooping
#

```

- Device B:

```

#
stp region-configuration
 region-name example
 active region-configuration
#
 stp enable
#
 stp config-digest-snooping
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 stp config-digest-snooping
#

```

## Example: Configuring interoperability with an upstream third-party device that uses a private MSTP implementation

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

The designated port of an RSTP, PVST, or MSTP device can implement rapid state transition through exchanging Proposal and Agreement packets with the root port of a downstream device.

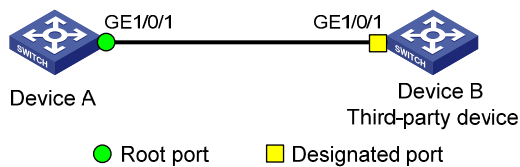
When the downstream device is an HP device and is connected to a third-party upstream device that has a private spanning tree implementation, the rapid state transition implementation might be limited.

As shown in [Figure 208](#):

- Device A is an HP device.
- Device A connects to a third-party device (Device B) that has a private spanning tree implementation.
- Device A and Device B are in the same MST region, and Device B is the root bridge.

Enable No Agreement Check on the port connecting Device A to Device B, so that port GigabitEthernet 1/0/1 on Device B can rapidly transit its port state.

**Figure 208 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 enable
```

6. Perform an mCheck operation globally to make sure all ports of Device A are operating in MSTP mode.

```
[DeviceA] stp 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 GigabitEthernet 1/0/1 of Device A.

```
<DeviceA> system-view
```

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

```
[DeviceA-GigabitEthernet1/0/1] stp no-agreement-check
```

## Verifying the configuration

# 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

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

Device A:

```
#
stp region-configuration
 region-name example
 active region-configuration
#
stp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 stp no-agreement-check
#
```

# SSH configuration examples

This chapter provides examples for configuring SSH for secure remote access and file transfer.

## General configuration restrictions and guidelines

When acting as an SSH server, the switch supports SSH2.0 and SSH1. When acting as an SSH client, the switch supports SSH2.0 only.

## Example: Configuring the switch as an Stelnet server for password authentication

### Applicable product matrix

| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

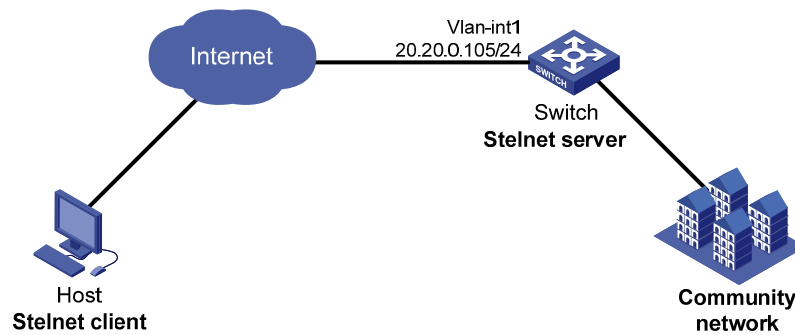
### Network requirements

As shown in [Figure 209](#), 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 authentication and the method is password authentication.

The switch limits the number of authentication attempts to prevent malicious hacking of usernames and passwords.

Figure 209 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.
- When password authentication is used, the command level accessible to the user is authorized by AAA.
- Authentication fails if the total number of authentication attempts (including both publickey and password authentication) exceeds the upper limit configured by the **ssh server authentication-retries** command. This configured upper limit takes effect only on the users at next login.

## Configuration procedures

### Configuring the switch

# Assign an IP address to VLAN interface 1. The Stelnet client uses the IP address as the destination address of the SSH connection.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 20.20.0.105 255.255.255.0
[Switch-Vlan-interface1] quit
```

# Generate RSA and DSA key pairs.

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

```

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

Enable the SSH server function.
[Switch] ssh server enable
Info: Enable SSH server

Set the maximum number of SSH authentication attempts to 5.
[Switch] ssh server authentication-retries 5

Set the authentication mode 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

Create a local user client001.
[Switch] local-user client001
New local user added.

Set the password as aabbcc for the local user client001.
[Switch-luser-client001] password simple aabbcc

Specify the service type as ssh for the local user client001.
[Switch-luser-client001] service-type ssh

Set the user privilege level to 3 for the local user client001.
[Switch-luser-client001] authorization-attribute level 3
[Switch-luser-client001] quit

Create an SSH user client001. Specify the service type as Stelnet and the authentication method as password for the user.
[Switch] ssh user client001 service-type stelnet authentication-type password

```

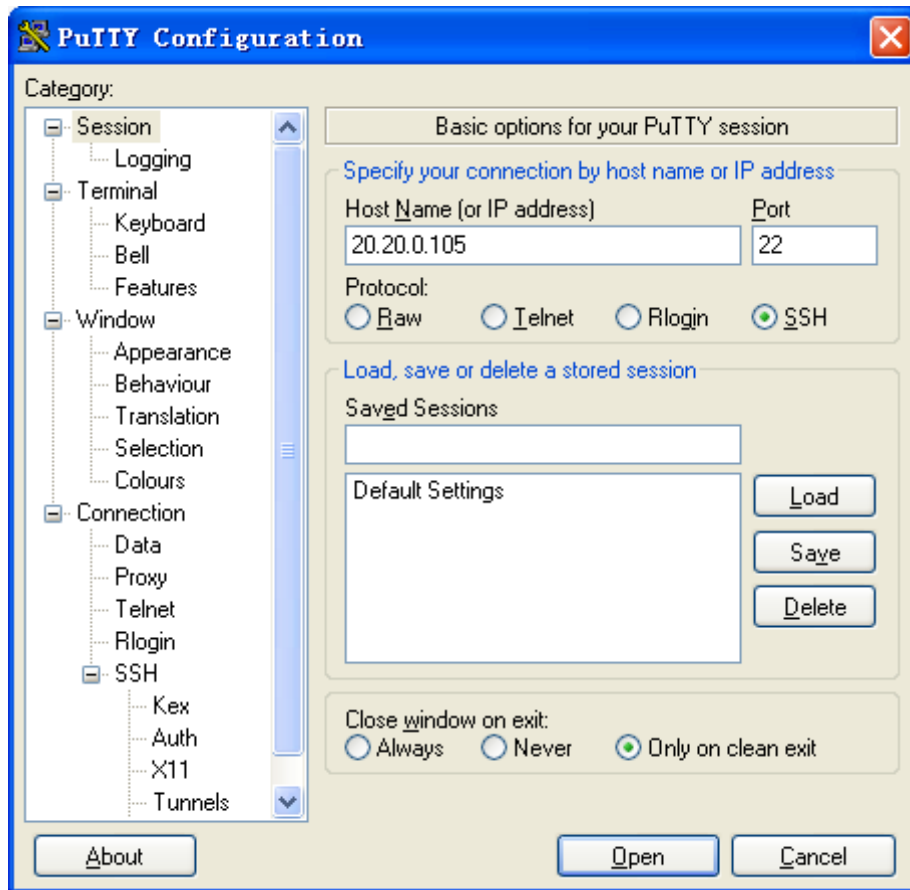
## Configuring the SSH client

There are different types of Stelnet client software, such as PuTTY and OpenSSH. This example uses an Stelnet client that runs PuTTY version 0.58.

To establish a connection to the Stelnet server:

1. Launch PuTTY.exe to enter the interface as shown in Figure 210.
2. In the **Host Name (or IP address)** field, enter the IP address **20.20.0.105** of the Stelnet server.

Figure 210 Specifying the Stelnet server



3. Click **Open**.  
A security alert window 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>

## Configuration files

```
#
vlan 1
#
local-user client001
password cipher c3$6XrvmIWDHxv6M9ykP9qJrqy9/J1b1z8xSg==
authorization-attribute level 3
service-type ssh
#
interface Vlan-interface1
ip address 20.20.0.105 255.255.255.0
#
ssh server enable
ssh server authentication-retries 5
ssh user client001 service-type stelnet authentication-type password
#
user-interface vty 0 15
authentication-mode scheme
user privilege level 3
protocol inbound ssh
#
```

## Example: Configuring the switch as an Stelnet server for publickey authentication

### Applicable product matrix

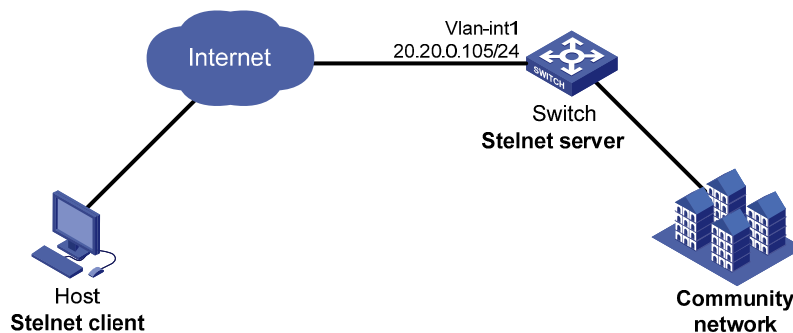
| Product series | Software version |
|----------------|------------------|
| HP 5500 EI     | Release 2220     |
| HP 5500 SI     |                  |

## Network requirements

As shown in [Figure 211](#), you can log in to the switch through the Stelnet client that runs on the host for configuration and management.

The switch acts as the Stelnet server, and uses publickey authentication and the RSA public key algorithm.

**Figure 211 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 generate RSA key pairs on the server.

## Configuration restrictions and guidelines

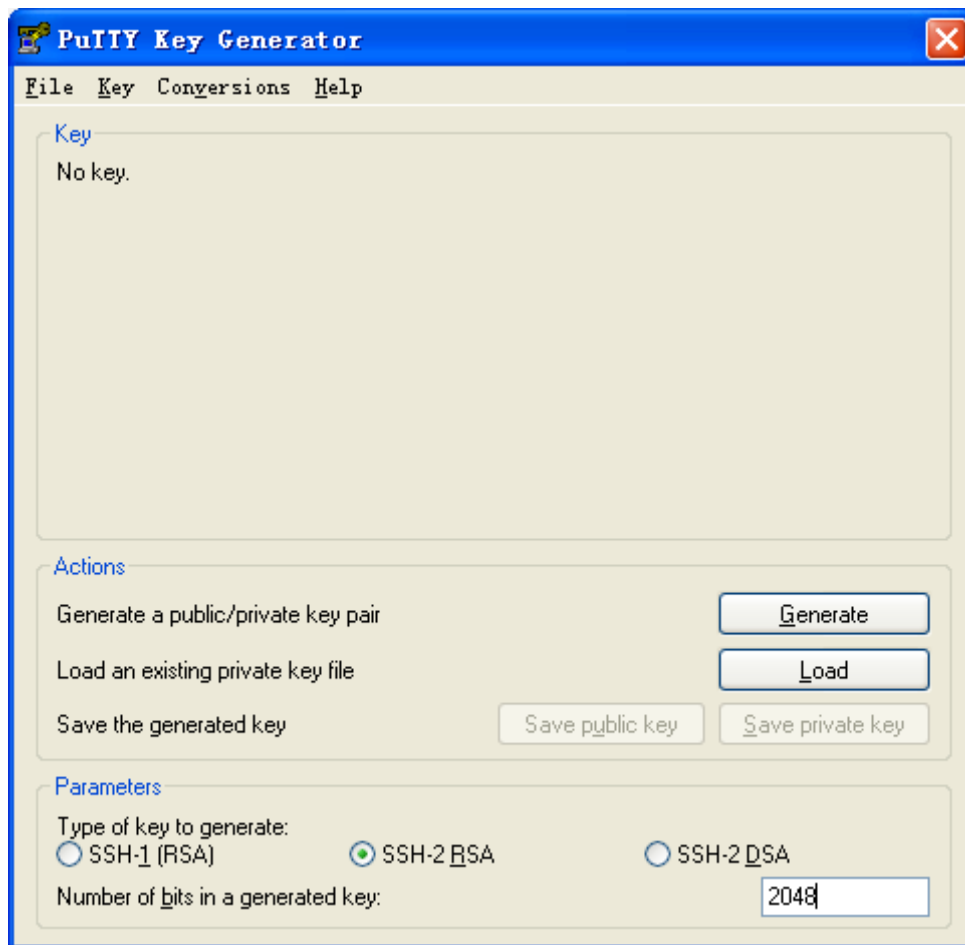
When publickey authentication is used, the command level accessible to the user is set by the **user privilege level** command on the user interface.

## Configuration procedures

### Configuring the Stelnet client

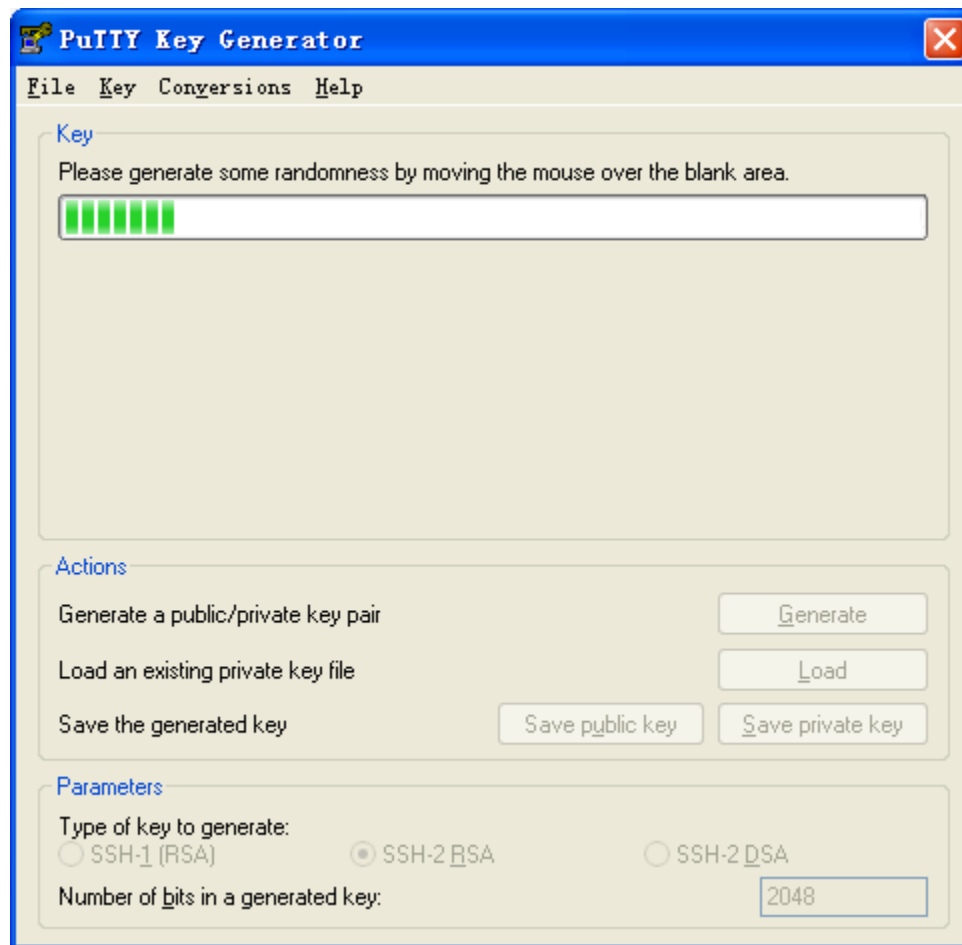
1. Run PuTTYGen.exe on the client to enter the interface as shown in [Figure 212](#).
2. Select **SSH-2 RSA** and enter **2048** in the **Number of bits in a generated key** field.
3. Click **Generate**.

Figure 212 Generating the RSA key pair on the client



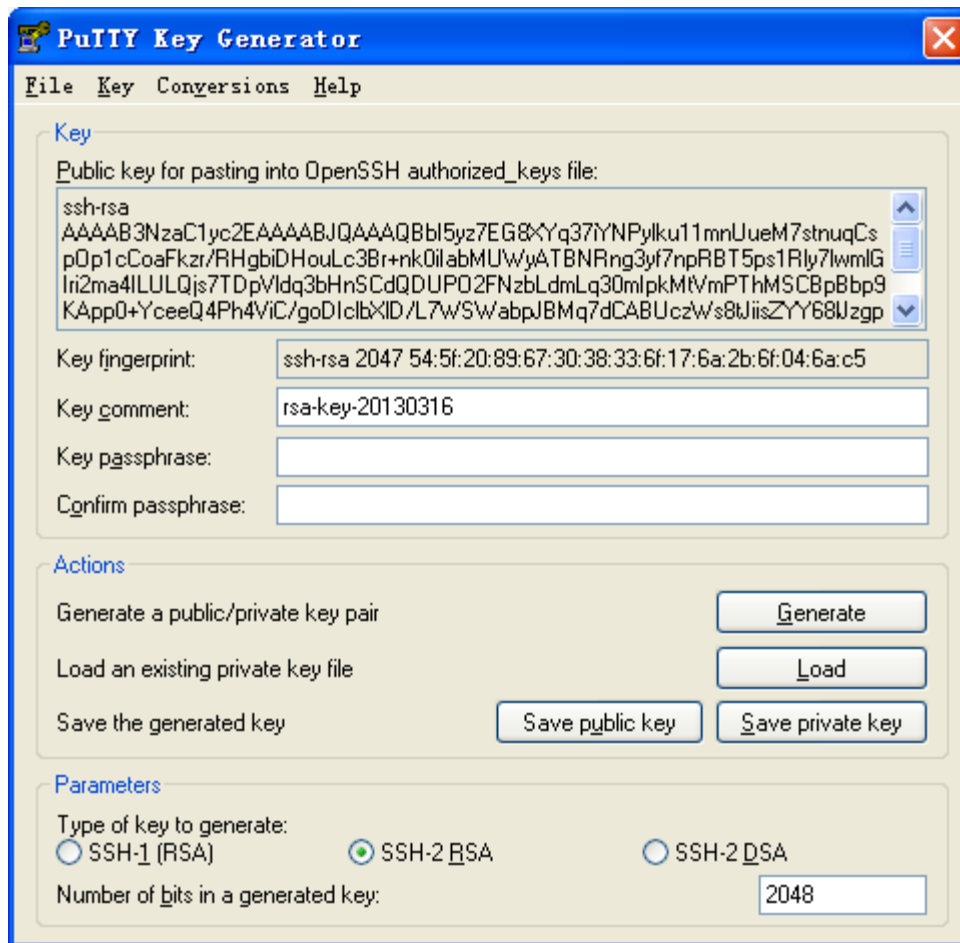
4. Continuously move the mouse and do not place the mouse over the progress bar shown in [Figure 213](#). Otherwise, the key pair generating progress stops.

Figure 213 Generating process



5. Save the public key after the key pair is generated:
  - a. Click **Save public key**.
  - b. Specify a directory (root directory of disk C in this example).
  - c. Enter a file name (**key.pub** in this example).
  - d. Click **Save**.

Figure 214 Saving the generated key pair



6. Click **Save private key** to save the private key.  
A confirmation dialog box appears.
7. Click **Yes**, enter a file name (**private.ppk** in this example), and click **Save**.

### Configuring the switch as an FTP server

# Assign an IP address to VLAN interface 1.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 20.20.0.105 255.255.255.0
[Switch-Vlan-interface1] quit
```

# Create a local user **ftp** on the switch.

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

# Set the password to **ftp** for the local user **ftp**.

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

# Set the user privilege level to **3** for the local user **ftp**.

```
[Switch-luser-ftp] authorization-attribute level 3
```

```

Assign the working directory flash:/ to the local user ftp.
[Switch-luser-ftp] authorization-attribute work-directory flash:/

Specify the service type as ftp for the local user ftp.
[Switch-luser-ftp] service-type ftp
[Switch-luser-ftp] quit

Enable the FTP server function on the switch.
[Switch] ftp server enable
[Switch] quit

```

## Uploading the public key file to the server

```

Log in to the switch from the client and upload the public key file (key.pub) to the switch through FTP.
c:\> ftp 20.20.0.105
Connected to 20.20.0.105.
220 FTP service ready.
User(20.20.0.105:(none)):ftp
331 Password required for ftp.
Password:
230 User logged in.
ftp> put key.pub
200 Port command okay.
150 Opening ASCII mode data connection for /key.pub.
226 Transfer complete.
ftp> bye
221 Server closing.
c:\

```

## Configuring the switch as an Stelnet server

```

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

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

Set the user privilege level to 3.
[Switch-ui-vty0-15] user privilege level 3
[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 user client002.
[Switch] local-user client002
New local user added.

Specify the service type as ssh for the local user client002.
[Switch-luser-client002] service-type ssh

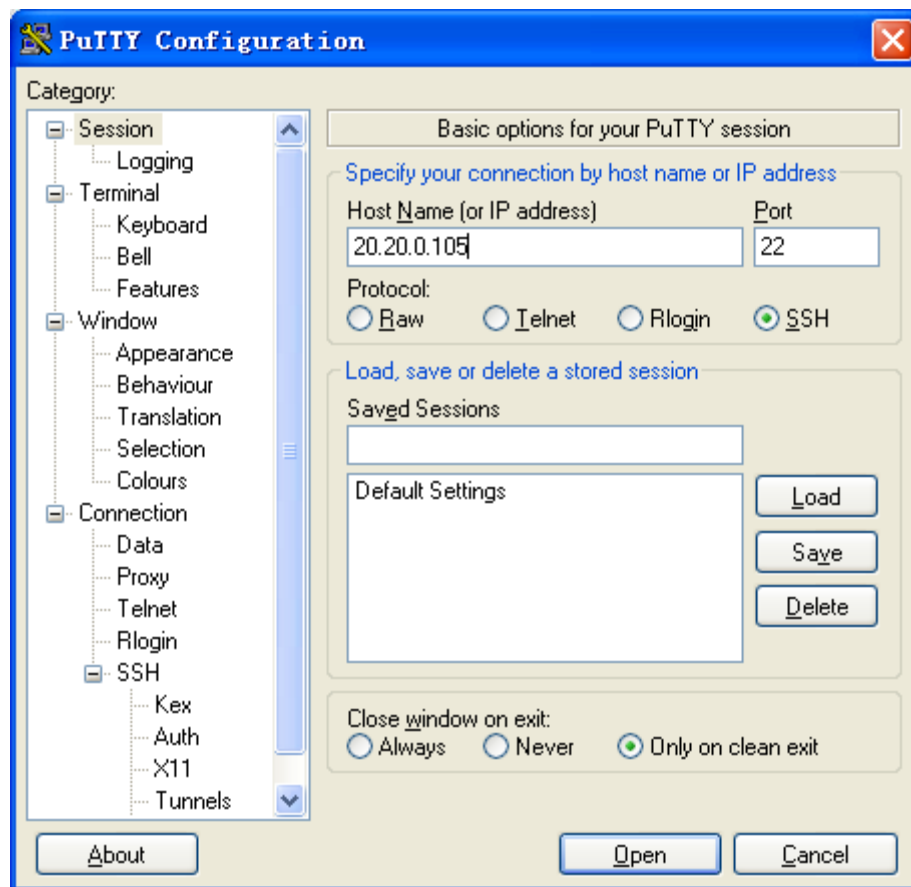
Set the user privilege level to 3 for the local user client002.
[Switch-luser-client002] authorization-attribute level 3
[Switch-luser-client002] quit

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 as shown in [Figure 215](#).
2. In the **Host Name (or IP address)** field, enter the IP address **20.20.0.105** of the Stelnet server.

Figure 215 Specifying the Stelnet server



3. Select **Connection** > **SSH** > **Auth** from the navigation tree.

The window as shown in [Figure 216](#) appears.

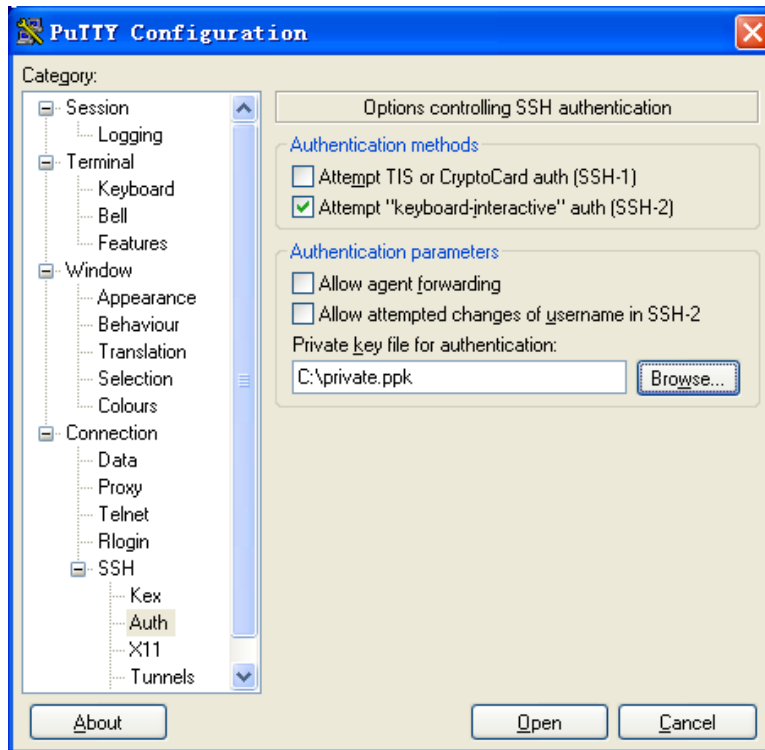
4. Click **Browse....**

A file selection window appears.

5. Select the private key file (**private.ppk** in this example) and click **OK**.



Figure 216 Specifying the private key file



6. Click **Open** to connect to the server.
7. Enter the username **client002** to log in to the Stelnet server.

## Verifying the configuration

# Verify that you can use the username **client002** to access the Stelnet server's CLI.

```
Login as: client002
```

```
Authenticating with public key "rsa-key-20130316"
```

```

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

```

```
<Switch>
```

## Configuration files

```
#
vlan 1
#
public-key peer Switch001
```

```

 public-key-code begin
30819D300D06092A864886F70D010101050003818B0030818702818100A2DBC1FD76A837BEF5D32259844
2D6753B2E8F7ADD6D6209C80843B206B309078AFE2416CB4FAD496A6627243EAD766D57AEA70B901B4B45
66D9A651B133BAE34E9B9F04E542D64D0E9814D7E3CBCDBCAF28FF21EE4EADAE6DF52001944A40414DFF2
80FF043B14838288BE7F9438DC71ABBC2C28BF78F34ADF3D1C912579A19020125
 public-key-code end
peer-public-key end
#
local-user client002
 authorization-attribute level 3
 service-type ssh
#
local-user ftp
 password cipher c3$sg9Wgq0lw8vnAv2FKGTOYgFJm3nn2w==
 authorization-attribute work-directory flash:/
 authorization-attribute level 3
 service-type ftp
#
interface Vlan-interface1
 ip address 20.20.0.105 255.255.255.0
#
ssh server enable
ssh user client002 service-type stelnet authentication-type publickey assign publickey
Switch001
#
user-interface vty 0 15
 authentication-mode scheme
 user privilege level 3
 protocol inbound ssh
#

```

## Example: Configuring the switch as an Stelnet client for password authentication

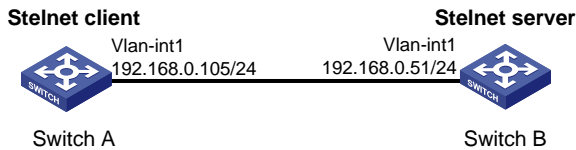
### Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

# Network requirements

As shown in [Figure 217](#), you can log in to Switch B through the Stelnet client that runs on Switch A for configuration and management. Switch B acts as the Stelnet server and uses password authentication and DSA public key algorithm.

**Figure 217 Network diagram**



# Requirements analysis

To enable the client to access the server if the first-time authentication is disabled, you must perform the following tasks on the client:

1. Configure the server's host public key.
2. Specify the public key name for authentication.

# Configuration procedures

## Configuring Switch B

# Assign an IP address to VLAN interface 1.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 192.168.0.51 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

# Generate a DSA key pair.

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

# Display the DSA key pair on Switch B.

```
[SwitchB] display public-key local dsa public
```

```

=====
Time of Key pair created: 15:23:11 2012/02/26
Key name: HOST_KEY
Key type: DSA Encryption Key
=====
Key code:
3082033B3082022E06072A8648CE380401308202210282010100F13ACC1693AFD04B9E1E8D2A9DEA
6DE8DE4C276BE2BF15B6CFF6E269B0169378CB0DDDE23D187827015DC67E6768193914B823BDF215
D0DAD7A151E434F9E128DAFB9DEF07874621E70D7FC4577D2851C707BC86AC0FD3829B862C5CD7
003334E3BBF36FD48D54766638788B790AAC6451407281A3694D6B74DA31DA0415264F3FA3E1A6E0
F57002C0FAEF46F15545242D323BF0ED85A3365F00702CBDE794C09A6C7DDE05F1E0E928E82EEA31
DB2454CD2E6866599DDF2381163734AD5C6F8A98A791BAD8942A5D12D674FCA42EA93FF7FDD23E4E
E29C35F75C8E52EF1B132073679EE2E62DF435CE35BB7F0FB756DF92A95C3652F979BD03F8D2BB62
018B021500C773218C737EC8EE993B4F2DED30F48EDACE915F0282010100D43E90A700F70A4EE08C
728A297DA04566A0A112DC49ABF51A37BBB56BFE518BBD71359EACE98712BEC58A261FC6D5FE78
B9A67ED494288CB5A1984CA67037A16BFC75B889829C92465BA094460D7EEF918969C0ADAE4841D1
4A880142151C394C28F2731304C456350479D62014C81F07A0BA5FD0F9301D8F9AF9F30C6D21471F
00B65714991F96E34328798FBFBAAA1A64A74EA05DFA2CA0035F2A94C2EBCE7D283D144D4F5B5B61
B4ED74E9A10E375FFE2FA9D2D41B889D36620183637A77D328C67C2196ABA36E3DAE08B774836A3B
5D3BFD059A967F95A00863A1660EB59F9AAD7F470D14F3D174DB51885E6B430B003ACDEB6C9B213A
8749765992E40382010500028201005B7C602A155775741EAAC552562B46D766D9917946D9C66E09
509BBB26E6A05EA5E45B95A797ED59E7BA6F06E15B3355A472DF734D625F4BFD41D9F3FF52F48D0E
D17285E70EF203D4EB97C915D5AEF2EE32F3F00BC742D080E7635AB49EF3624F6AB27E3270E082B8
C7FD5E0610259993D931719F5D6A8165A62E209A1734242C5E161AC68B5670F8CA58BF7C6ED25E79
812DAE633EB94C5A9E9614777FB7038A200965266E46145173C8EA9EB91C35550A335F6E7E4C1FBD
2D43E67CC7422E3D4D6AE931A4AD817335600BD76642196568013BDCC98973E57EE281004BEC7539
8559E27FE893A6F3BC1E11ACDB1DB4453343B0219A8C6D15AB280EFFB05F37

```

# 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
```

# Enable the user interfaces to support SSH.

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

# Create a local user **client001**.

```
[SwitchB] local-user client001
New local user added.
```

# Set the password to **aabbcc** for the local user **client001**.

```
[SwitchB-luser-client001] password simple aabbcc
```

# Specify the service type as **ssh** for the local user **client001**.

```
[SwitchB-luser-client001] service-type ssh
```

# Set the user privilege level to **3** for the local user **client001**.

```
[SwitchB-luser-client001] authorization-attribute level 3
[SwitchB-luser-client001] quit
```

# Create an SSH user. Specify the service type as **Stelnet** and the authentication method as **password** for the user.

```
[SwitchB] ssh user client001 service-type stelnet authentication-type password
```

## Configuring Switch A

# Assign an IP address to VLAN interface 1.

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

If first-time authentication is enabled, the configuration on Switch A is completed. You can establish a connection with the server from the client.

If first-time authentication is disabled, proceed with the following configurations:

# Enter public key view.

```
[SwitchA] public-key peer key1
Public key view: return to System View with "peer-public-key end".
```

# Enter public key code view.

```
[SwitchA-pkey-public-key] public-key-code begin
Public key code view: return to last view with "public-key-code end".
```

# Enter the host public key of the SSH server. (You can obtain the server's host public key by using the **display public-key local dsa public** command on the server.)

```
[SwitchA-pkey-key-code]3082033B3082022E06072A8648CE380401308202210282010100F13ACC169
3AFD04B9E1E8D2A9DEA
[SwitchA-pkey-key-code]6DE8DE4C276BE2BF15B6CFF6E269B0169378CB0DDDE23D187827015DC67E6
768193914B823BDF215
[SwitchA-pkey-key-code]D0DAD7A151E434F9E128DAFB9DEF9AE07874621E70D7FC4577D2851C707BC8
6AC0FD3829B862C5CD7
[SwitchA-pkey-key-code]003334E3BBF36FD48D54766638788B790AAC6451407281A3694D6B74DA31D
A0415264F3FA3E1A6E0
[SwitchA-pkey-key-code]F57002C0FAEF46F15545242D323BF0ED85A3365F00702CBDE794C09A6C7DD
E05F1E0E928E82EEA31
[SwitchA-pkey-key-code]DB2454CD2E6866599DDF2381163734AD5C6F8A98A791BAD8942A5D12D674F
CA42EA93FF7FDD23E4E
[SwitchA-pkey-key-code]E29C35F75C8E52EF1B132073679EE2E62DF435CE35BB7F0FB756DF92A95C3
652F979BD03F8D2BB62
[SwitchA-pkey-key-code]018B021500C773218C737EC8EE993B4F2DED30F48EDACE915F0282010100D
43E90A700F70A4EE08C
[SwitchA-pkey-key-code]728A297DA04566A0A112DC49ABF51A37BBB56BFE518BBD71359EACE9871
2BEC58A261FC6D5FE78
[SwitchA-pkey-key-code]B9A67ED494288CB5A1984CA67037A16BFC75B889829C92465BA094460D7EE
F918969C0ADAE4841D1
[SwitchA-pkey-key-code]4A880142151C394C28F2731304C456350479D62014C81F07A0BA5FD0F9301
D8F9AF9F30C6D21471F
[SwitchA-pkey-key-code]00B65714991F96E34328798FBFBAAA1A64A74EA05DFA2CA0035F2A94C2EBC
```

```

E7D283D144D4F5B5B61
[SwitchA-pkey-key-code]B4ED74E9A10E375FFE2FA9D2D41B889D36620183637A77D328C67C2196ABA
36E3DAE08B774836A3B
[SwitchA-pkey-key-code]5D3BFD059A967F95A00863A1660EB59F9AAD7F470D14F3D174DB51885E6B4
30B003ACDEB6C9B213A
[SwitchA-pkey-key-code]8749765992E40382010500028201005B7C602A155775741EAAC552562B46D
766D9917946D9C66E09
[SwitchA-pkey-key-code]509BBB26E6A05EA5E45B95A797ED59E7BA6F06E15B3355A472DF734D625F4
BFD41D9F3FF52F48D0E
[SwitchA-pkey-key-code]D17285E70EF203D4EB97C915D5AEF2EE32F3F00BC742D080E7635AB49EF36
24F6AB27E3270E082B8
[SwitchA-pkey-key-code]C7FD5E061025993D931719F5D6A8165A62E209A1734242C5E161AC68B567
0F8CA58BF7C6ED25E79
[SwitchA-pkey-key-code]812DAE633EB94C5A9E9614777FB7038A200965266E46145173C8EA9EB91C3
5550A335F6E7E4C1FBD
[SwitchA-pkey-key-code]2D43E67CC7422E3D4D6AE931A4AD817335600BD76642196568013BDCC9897
3E57EE281004BEC7539
[SwitchA-pkey-key-code]8559E27FE893A6F3BC1E11ACDB1DB4453343B0219A8C6D15AB280EFFB05F3
7

Return to public key view and save the host public key.
[SwitchA-pkey-key-code] public-key-code end

Return to system view.
[SwitchA-pkey-public-key] peer-public-key end

Specify the host public key name of the Stelnet server (192.168.0.51) as key1.
[SwitchA] ssh client authentication server 192.168.0.51 assign publickey key1
[SwitchA] quit

```

## Verifying the configuration

# If first-time authentication is enabled, verify that you can log in to Switch B after entering the correct password. The client saves the server's host public key locally.

```

<SwitchA> ssh 192.168.0.51
Username: client001
Trying 192.168.0.51 ...
Press CTRL+K to abort
Connected to 192.168.0.51 ...

```

```

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter password:

```

```

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

```

<SwitchB>

# If first-time authentication is disabled, verify that you can log in to Switch B after entering the correct password.

<SwitchA> ssh2 192.168.0.51

Username: client001

Trying 192.168.0.51

Press CTRL+K to abort

Connected to 192.168.0.51...

Enter password:

```

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

```

<SwitchB>

## Configuration files

- Switch A:

```
#
vlan 1
#
public-key peer key1
public-key-code begin
 3082033B3082022E06072A8648CE380401308202210282010100F13ACC1693AFD04B9E1E8D
 2A9DEA6DE8DE4C276BE2BF15B6CFF6E269B0169378CB0DDDE23D187827015DC67E67681939
 14B823BDF215D0DAD7A151E434F9E128DAFB9DEFAE07874621E70D7FC4577D2851C707BC86
 AC0FD3829B862C5CD7003334E3BBF36FD48D54766638788B790AAC6451407281A3694D6B74
 DA31DA0415264F3FA3E1A6E0F57002C0FAEF46F15545242D323BF0ED85A3365F00702CBDE7
 94C09A6C7DDE05F1E0E928E82EEA31DB2454CD2E6866599DDF2381163734AD5C6F8A98A791
 BAD8942A5D12D674FCA42EA93FF7FDD23E4EE29C35F75C8E52EF1B132073679EE2E62DF435
 CE35BB7F0FB756DF92A95C3652F979BD03F8D2BB62018B021500C773218C737EC8EE993B4F
 2DED30F48EDACE915F0282010100D43E90A700F70A4EE08C728A297DA04566A0A112DC49AB
 F51A37BBB5BFE518BBD71359EACE98712BEC58A261FC6D5FE78B9A67ED494288CB5A198
 4CA67037A16BFC75B889829C92465BA094460D7EEF918969C0ADAE4841D14A880142151C39
 4C28F2731304C456350479D62014C81F07A0BA5FD0F9301D8F9AF9F30C6D21471F00B65714
 991F96E34328798FBFBAAA1A64A74EA05DFA2CA0035F2A94C2EBCE7D283D144D4F5B5B61B4
 ED74E9A10E375FFE2FA9D2D41B889D36620183637A77D328C67C2196ABA36E3DAE08B77483
 6A3B5D3BFD059A967F95A00863A1660EB59F9AAD7F470D14F3D174DB51885E6B430B003ACD
 EB6C9B213A8749765992E40382010500028201005B7C602A155775741EAAC552562B46D766
 D9917946D9C66E09509BBB26E6A05EA5E45B95A797ED59E7BA6F06E15B3355A472DF734D62
 5F4BFD41D9F3FF52F48D0ED17285E70EF203D4EB97C915D5AEF2EE32F3F00BC742D080E763
 5AB49EF3624F6AB27E3270E082B8C7FD5E0610259993D931719F5D6A8165A62E209A173424
 2C5E161AC68B5670F8CA58BF7C6ED25E79812DAE633EB94C5A9E9614777FB7038A20096526
 6E46145173C8EA9EB91C35550A335F6E7E4C1FBD2D43E67CC7422E3D4D6AE931A4AD817335
```

```

600BD76642196568013BDCC98973E57EE281004BEC75398559E27FE893A6F3BC1E11ACDB1D
B4453343B0219A8C6D15AB280EFFB05F37
public-key-code end
peer-public-key end
#
interface Vlan-interface1
ip address 192.168.0.105 255.255.255.0
#
ssh client authentication server 192.168.0.51 assign publickey key1
#

```

- Switch B:

```

#
vlan 1
#
local-user client001
password cipher c3$G+xmuBmDrurppAOsyNcYNzNqB+C/NSFsPg==
authorization-attribute level 3
service-type ssh
#
interface Vlan-interface1
ip address 192.168.0.51 255.255.255.0
#
ssh server enable
ssh user client001 service-type stelnet authentication-type password
#
user-interface vty 0 15
authentication-mode scheme
user privilege level 3
protocol inbound ssh
#

```

## Example: Configuring the switch as an SFTP client for publickey authentication

### Applicable product matrix

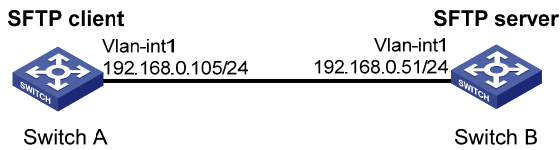
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	



# Network requirements

As shown in [Figure 218](#), you can log in to Switch B through the SFTP client that runs on Switch A for file management and transfer. Switch B acts as the SFTP server and uses publickey authentication and DSA public key algorithm.

**Figure 218 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 generate a DSA key pair on Switch B.

# Configuration procedures

## Configuring Switch A as an SFTP client

```
Assign an IP address to VLAN interface 1.
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.0.105 255.255.255.0
[SwitchA-Vlan-interface1] quit

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

```

+++++
+++++
+++++
+++++

Export the DSA host public key to the file key2.pub.
[SwitchA] public-key local export dsa ssh2 key2.pub
..
[SwitchA] quit

```

## Configuring Switch B as an FTP server

```

Assign an IP address to VLAN interface 1.
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 192.168.0.51 255.255.255.0
[SwitchB-Vlan-interface1] quit

Create a local user ftp.
[SwitchB] local-user ftp
New local user added.

Set the password to ftp for the user ftp.
[SwitchB-luser-ftp] password simple ftp

Set the user privilege level to 3 for the user ftp.
[SwitchB-luser-ftp] authorization-attribute level 3

Assign the working directory flash:/ to the user ftp.
[SwitchB-luser-ftp] authorization-attribute work-directory flash:/

Specify the service type as ftp for the user ftp.
[SwitchB-luser-ftp] service-type ftp
[SwitchB-luser-ftp] quit

Enable the FTP server function on Switch B.
[SwitchB] ftp server enable
[SwitchB] quit

```

## Uploading the public key file to the server

```

Log in to the FTP server from Switch A and upload the public key file to the server.
<SwitchA> ftp 192.168.0.51
Trying 192.168.0.51 ...
Press CTRL+K to abort
Connected to 192.168.0.51.
220 FTP service ready.
User(192.168.0.51:(none)):ftp
331 Password required for ftp.
Password:
230 User logged in.

[ftp]put key2.pub

```

```
227 Entering Passive Mode (192,168,0,51,8,157).
125 ASCII mode data connection already open, transfer starting for /key2.pub.
226 Transfer complete.
FTP: 1187 byte(s) sent in 0.206 second(s), 5.00Kbyte(s)/sec.
```

```
[ftp] quit
```

## Configuring Switch B as the SFTP server

# Generate a DSA public key pair.

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

# Enable the SSH server function

```
[SwitchB] ssh server enable
```

# Enable the SFTP server.

```
[SwitchB] sftp 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
```

# Enable the user interfaces to support SSH.

```
[SwitchB-ui-vty0-15] protocol inbound ssh
```

[# Set the user privilege level to **3**.

```
SwitchB-ui-vty0-15] user privilege level 3
[SwitchB-ui-vty0-15] quit
```

# Import the peer public key from the file **key2.pub**.

```
[SwitchB] public-key peer Switch001 import sshkey key2.pub
```

# Create a local user **client002**.

```
[SwitchB] local-user client002
New local user added.
```

# Specify the service type as **ssh** for the local user **client002**.

```
[SwitchB-luser-client002] service-type ssh
```

# Set the user privilege level to **3** for local user **client002**.

```
[SwitchB-luser-client002] authorization-attribute level 3
[SwitchB-luser-client002] quit
```

# Create an SSH user **client002**. Specify the service type as **sftp** and authentication method as **publickey** for the user **client002**. 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
Input Username: client002
Trying 192.168.0.51 ...
Press CTRL+K to abort
Connected to 192.168.0.51 ...
```

```
The Server is not authenticated. Continue? [Y/N]:y
```

```
Do you want to save the server public key? [Y/N]:n
```

```
sftp-client>
```

# Display files under the current directory of the server.

```
sftp-client> dir
-rwxrwxrwx 1 noone nogroup 5268 Apr 26 23:50 startup.cfg
-rwxrwxrwx 1 noone nogroup 13138750 Apr 26 13:52 switchB.bin
drwxrwxrwx 1 noone nogroup 0 Apr 26 12:00 seclog
-rwxrwxrwx 1 noone nogroup 4666612 Apr 26 14:25 switchB.btm
-rwxrwxrwx 1 noone nogroup 287 Apr 26 23:50 system.xml
-rwxrwxrwx 1 noone nogroup 1187 Apr 26 15:06 key2.pub
sftp-client>
```

# Add a directory named **new1** and verify the result.

```
sftp-client> mkdir new1
New directory created
sftp-client> dir
-rwxrwxrwx 1 noone nogroup 5268 Apr 26 23:50 startup.cfg
-rwxrwxrwx 1 noone nogroup 13138750 Apr 26 13:52 switchB.bin
drwxrwxrwx 1 noone nogroup 0 Apr 26 12:00 seclog
-rwxrwxrwx 1 noone nogroup 4666612 Apr 26 14:25 switchB.btm
-rwxrwxrwx 1 noone nogroup 287 Apr 26 23:50 system.xml
-rwxrwxrwx 1 noone nogroup 1187 Apr 26 15:06 key2.pub
drwxrwxrwx 1 noone nogroup 0 Apr 26 15:16 new1
```

# Rename directory **new1** to **new2** and verify the result.

```
sftp-client> rename new1 new2
File successfully renamed
sftp-client> dir
-rwxrwxrwx 1 noone nogroup 5268 Apr 26 23:50 startup.cfg
-rwxrwxrwx 1 noone nogroup 13138750 Apr 26 13:52 switchB.bin
```

```

drwxrwxrwx 1 noone nogroup 0 Apr 26 12:00 seclog
-rwxrwxrwx 1 noone nogroup 466612 Apr 26 14:25 switchB.btm
-rwxrwxrwx 1 noone nogroup 287 Apr 26 23:50 system.xml
-rwxrwxrwx 1 noone nogroup 1187 Apr 26 15:06 key2.pub
drwxrwxrwx 1 noone nogroup 0 Apr 26 15:16 new2

```

# Exit SFTP client view.

```

sftp-client> quit
Bye
Connection closed.
<SwitchA>

```

## Configuration files

- Switch A:

```

#
vlan 1
#
public-key peer Switch001
public-key-code begin
 3082033B3082022E06072A8648CE380401308202210282010100F13ACC1693AFD04B9E1E8D
 2A9DEA6DE8DE4C276BE2BF15B6CFF6E269B0169378CB0DDDE23D187827015DC67E67681939
 14B823BDF215D0DAD7A151E434F9E128DAFB9DEF07874621E70D7FC4577D2851C707BC86
 AC0FD3829B862C5CD7003334E3BBF36FD48D54766638788B790AAC6451407281A3694D6B74
 DA31DA0415264F3FA3E1A6E0F57002C0FAEF46F15545242D323BF0ED85A3365F00702CBDE7
 94C09A6C7DDE05F1E0E928E82EEA31DB2454CD2E6866599DDF2381163734AD5C6F8A98A791
 BAD8942A5D12D674FCA42EA93FF7FDD23E4EE29C35F75C8E52EF1B132073679EE2E62DF435
 CE35BB7F0FB756DF92A95C3652F979BD03F8D2BB62018B021500C773218C737EC8EE993B4F
 2DED30F48EDACE915F0282010100D43E90A700F70A4EE08C728A297DA04566A0A112DC49AB
 F51A37BBB56BFE518BBD71359EACE98712BEC58A261FC6D5FE78B9A67ED494288CB5A198
 4CA67037A16BFC75B889829C92465BA094460D7EEF918969C0ADAE4841D14A880142151C39
 4C28F2731304C456350479D62014C81F07A0BA5FD0F9301D8F9AF9F30C6D21471F00B65714
 991F96E34328798FBFBAAA1A64A74EA05DFA2CA0035F2A94C2EBCE7D283D144D4F5B5B61B4
 ED74E9A10E375FFE2FA9D2D41B889D36620183637A77D328C67C2196ABA36E3DAE08B77483
 6A3B5D3BFD059A967F95A00863A1660EB59F9AAD7F470D14F3D174DB51885E6B430B003ACD
 EB6C9B213A8749765992E40382010500028201001CBCFC26EBDF618121FA5B4934E0A591EC
 B11954AE88AE577A87866D2861B1DB8629B65BE2E2892455EF125A936528338375BF0CEA85
 F502FA2D0AA22675AE7908D06F34334FFE550B3D30EC28ABB668B0CAC9F8D26A198F4C8A0A
 DC086E9F8A30E8F8035B3949F6004F18A6DA21E7A1DBAE52F56ABFD5B9A32A52C6F43A272C
 9CAA7C751F0711BCECBE86BB16F0FC3939BD262B8732C6859156C456C01989EB37A275E8C9
 D4A2091433205693760557E3CA8A3CDA432856026C2F6279CC516CA84265CA63621DFB97A7
 2A40BC3C6DAD3A7D6DEDD3550293A81A36767C41501E7ECB217C85EC3779CAF0514C479A8D
 D476C2D4D1BE2A9D29F0206006CED45675
public-key-code end
peer-public-key end
#
interface Vlan-interface1
ip address 192.168.0.105 255.255.255.0

```

```
#
ssh user client002 service-type sftp authentication-type publickey
assign publickey Switch001
```

- Switch B:

```
#
ftp server enable
#
vlan 1
#
local-user client002
authorization-attribute level 3
service-type ssh
#
local-user ftp
password cipher c3$1KhVXwJ6k3Ms0RMDqHOYCEKHzhULw==
authorization-attribute work-directory flash:/
authorization-attribute level 3
service-type ftp
#
interface Vlan-interface1
ip address 192.168.0.51 255.255.255.0
#
user-interface vty 0 15
authentication-mode scheme
user privilege level 3
protocol inbound ssh
#
```

# Static multicast route configuration examples

This chapter provides static multicast route configuration examples.

Static multicast routes are used for RPF checks rather than multicast data forwarding.

## 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 connected to the neighbor.

## Example: Configuring static multicast routes (for changing RPF routes)

### Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

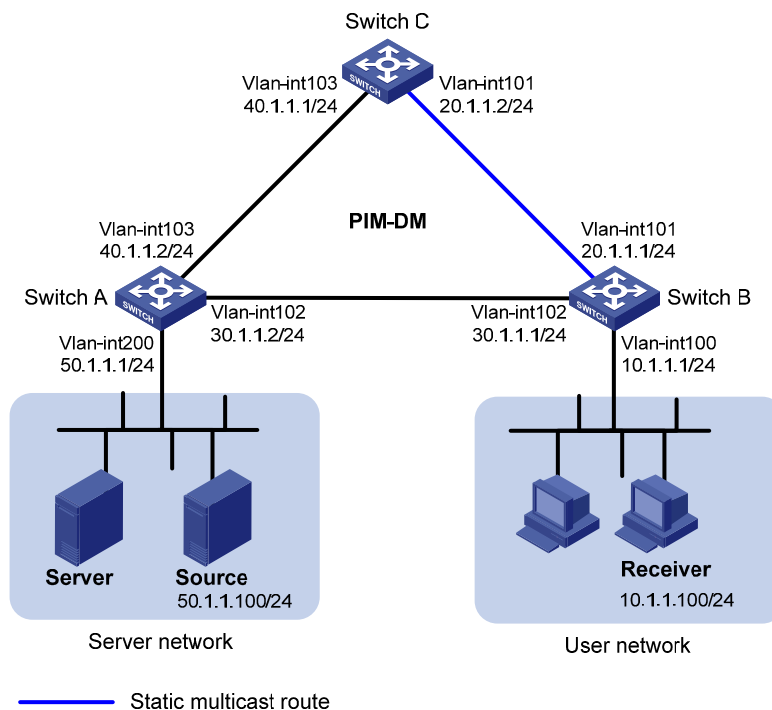
### Network requirements

As shown in [Figure 219](#):

- The server network and user network access the PIM-DM network through Switch A and Switch B.
- The server network sends large amount of unicast packets and multicast packets to the user network.
- All switches run OSPF, and they can communicate with each other through unicast routes.

To lessen the burden on unicast transmission path, configure a static multicast route on switch B. Multicast packets are then sent along a different path than that for unicast packets.

Figure 219 Network diagram



## Requirements analysis

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

1. Display the RPF neighbor information on Switch B to examine which RPF neighbor is used by the unicast route to the multicast source.
2. Configure a static multicast route to the multicast source with a different RPF neighbor than that of the unicast route.

## Configuration procedures

1. Configure the IP address and subnet mask for each interface as shown in Figure 219. (Details not shown.)
2. Enable OSPF on the switches in the PIM-DM domain. (Details not shown.)
3. Enable IP multicast routing, PIM-DM, and IGMP:

# 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 200
[SwitchA-Vlan-interface200] pim dm
[SwitchA-Vlan-interface200] quit
```



```
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim dm
[SwitchA-Vlan-interface102] quit
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim dm
[SwitchA-Vlan-interface103] quit

Enable IP multicast routing and PIM-DM on Switch C in the same way Switch A is configured.

On Switch B, enable IP multicast routing globally.
```

```
<SwitchB> system-view
[SwitchB] multicast routing-enable

Enable IGMP on VLAN-interface 100, and enable PIM-DM on each interface.
```

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] igmp enable
[SwitchB-Vlan-interface100] pim dm
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim dm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] pim dm
[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 to Source, and specify Switch C as its RPF neighbor.

```
[SwitchB] ip rpf-route-static 50.1.1.100 24 20.1.1.2
```

## Verifying the configuration

# On Switch B, 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 that:

- 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
igmp enable
pim dm
#
interface Vlan-interface101
ip address 20.1.1.1 255.255.255.0
pim dm
```

```

#
interface Vlan-interface102
 ip address 30.1.1.1 255.255.255.0
 pim dm
#
ospf 1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 20.1.1.0 0.0.0.255
 network 30.1.1.0 0.0.0.255
#
ip rpf-route-static 50.1.1.0 24 20.1.1.2
#

```

- Switch C:

```

#
 multicast routing-enable
#
 vlan 101
#
 vlan 103
#
 interface Vlan-interface101
 ip address 20.1.1.2 255.255.255.0.
 pim dm
#
 interface Vlan-interface103
 ip address 40.1.1.1 255.255.255.0
 pim dm
#
 ospf 1
 area 0.0.0.0
 network 20.1.1.0 0.0.0.255
 network 40.1.1.0 0.0.0.255
#

```

## Example: Configuring static multicast routes (for creating RPF routes)

### Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

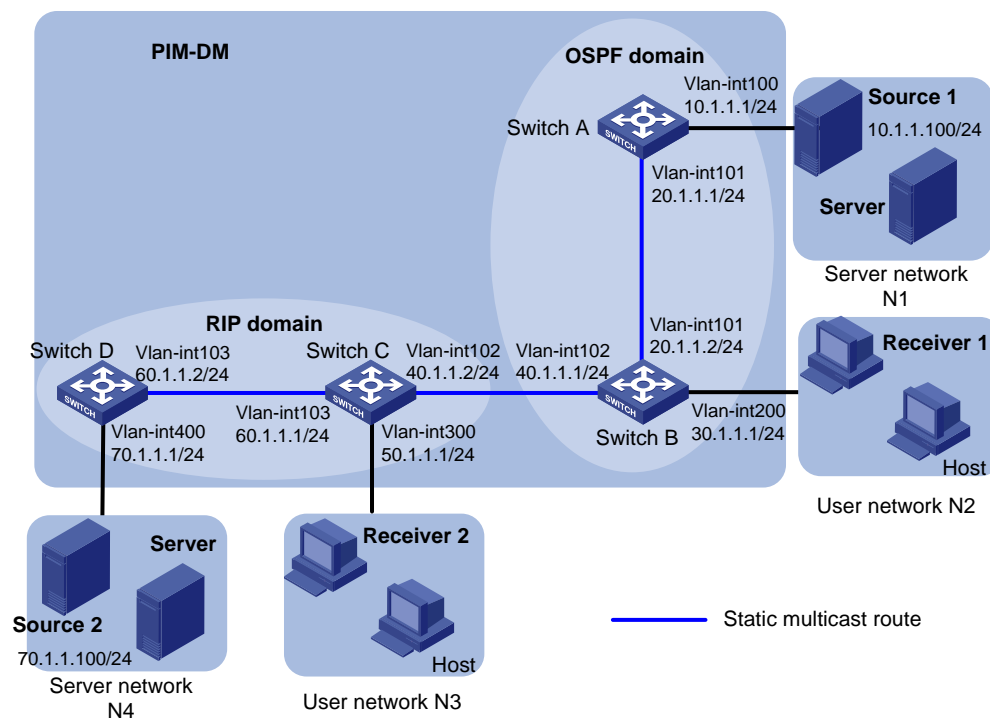
# Network requirements

As shown in Figure 220:

- 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 220 Network diagram



# Requirements analysis

To meet the network requirements, 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 220](#). (Details not shown.)
2. Enable OSPF on Switch A and Switch B. (Details not shown.)
3. Enable RIP on Switch C and Switch D. (Details not shown.)
4. Enable IP multicast routing, IGMP, and PIM-DM:

# On Switch A, enable IP multicast routing globally 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

Enable IGMP on VLAN-interface 200, and enable PIM-DM on each interface.
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp enable
[SwitchB-Vlan-interface200] pim dm
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim dm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] pim dm
[SwitchB-Vlan-interface102] quit
```

# Enable IP multicast routing, IGMP, and PIM-DM on Switch C in the same way Switch B is configured. (Details not shown.)

5. Display RPF routes:

# 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 because no RPF routes to Source 2 exist.

# 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 because no RPF routes to Source 1 exist.

## 6. Configure static multicast routes:

# On Switch B, configure a static multicast route, and specify Switch C as its RPF neighbor.

```
[SwitchB] ip rpf-route-static 70.1.1.100 24 40.1.1.2
```

# On Switch C, configure a static multicast route on Switch C, and specify Switch B as its RPF neighbor.

```
[SwitchC] ip rpf-route-static 10.1.1.100 24 40.1.1.1
```

## Verifying the configuration

# On Switch B, display information about the RPF route to Source 2.

```
[SwitchB] display multicast rpf-info 70.1.1.100
```

```
RPF information about source 70.1.1.100:
```

```
RPF interface: Vlan-interface102, RPF neighbor: 40.1.1.2
```

```
Referenced route/mask: 70.1.1.0/24
```

```
Referenced route type: multicast static
```

```
Route selection rule: preference-preferred
```

```
Load splitting rule: disable
```

# On Switch C, display information about the RPF route to Source 1.

```
[SwitchC] display multicast rpf-info 10.1.1.100
```

```
RPF information about source 10.1.1.100:
```

```
RPF interface: Vlan-interface101, RPF neighbor: 40.1.1.1
```

```
Referenced route/mask: 10.1.1.0/24
```

```
Referenced route type: multicast static
```

```
Route selection rule: preference-preferred
```

```
Load splitting rule: disable
```

The output shows that:

- The RPF routes to Source 2 and Source 1 are available on Switch B and Switch C, respectively.
- The RPF routes are the configured static multicast routes.

## Configuration files

- Switch A:

```
#
multicast routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
ip address 10.1.1.1 255.255.255.0.
pim dm
#
interface Vlan-interface101
ip address 20.1.1.1 255.255.255.0
```

```
pim dm
#
ospf 1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 20.1.1.0 0.0.0.255
#
```

- **Switch B:**

```
#
 multicast routing-enable
#
vlan 101 to 102
#
vlan 200
#
interface Vlan-interface101
 ip address 20.1.1.2 255.255.255.0.
 pim dm
#
interface Vlan-interface102
 ip address 40.1.1.1 255.255.255.0.
 pim dm
#
interface Vlan-interface200
 ip address 30.1.1.1 255.255.255.0
 igmp enable
 pim dm
#
ospf 1
 area 0.0.0.0
 network 20.1.1.0 0.0.0.255
 network 30.1.1.0 0.0.0.255
#
ip rpf-route-static 70.1.1.0 24 40.1.1.2
#
```

- **Switch C:**

```
#
 multicast routing-enable
#
vlan 102 to 103
#
vlan 300
#
interface Vlan-interface102
 ip address 40.1.1.2 255.255.255.0.
 pim dm
#
interface Vlan-interface103
```

```
ip address 60.1.1.1 255.255.255.0.
pim dm
#
interface Vlan-interface300
ip address 50.1.1.1 255.255.255.0
igmp enable
pim dm
#
rip 1
network 50.0.0.0
network 60.0.0.0
#
ip rpf-route-static 10.1.1.0 24 40.1.1.1
#
```

- Switch D:

```
#
multicast routing-enable
#
vlan 103
#
vlan 400
#
interface Vlan-interface103
ip address 60.1.1.2 255.255.255.0.
pim dm
#
interface Vlan-interface400
ip address 70.1.1.1 255.255.255.0
pim dm
#
rip 1
network 60.0.0.0
network 70.0.0.0
#
```



# Static routing configuration examples

This chapter provides static routing configuration examples.

## Example: Configuring basic static routing

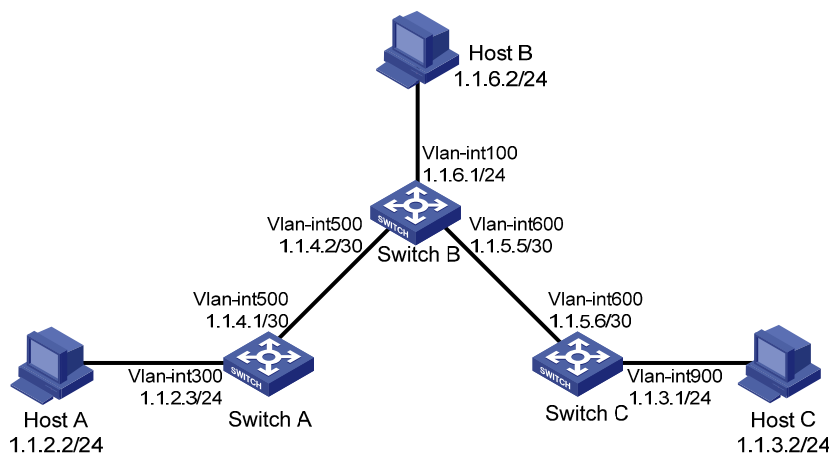
### Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

### Network requirements

As shown in [Figure 221](#), configure static routes on the switches for interconnections between any two hosts.

**Figure 221 Network diagram**



### Configuration procedures

1. Configure the IP address for interfaces:

# Configure IP addresses for interfaces on Switch A.

```
<SwitchA> system-view
[SwitchA] vlan 300
[SwitchA-Vlan300] interface Vlan-interface300
```

```
[SwitchA-Vlan-interface300] ip address 1.1.2.3 255.255.255.0
[SwitchA-Vlan-interface300] quit
[SwitchA] vlan 500
[SwitchA-Vlan500] interface Vlan-interface500
[SwitchA-Vlan-interface500] ip address 1.1.4.1 255.255.255.252
[SwitchA-Vlan-interface500] quit
```

#### # Configure IP addresses for interfaces on Switch B.

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-Vlan100] interface Vlan-interface100
[SwitchB-Vlan-interface100] ip address 1.1.6.1 255.255.255.0
[SwitchB-Vlan-interface100] quit
[SwitchB] vlan 500
[SwitchB-Vlan500] interface Vlan-interface500
[SwitchB-Vlan-interface500] ip address 1.1.4.2 255.255.255.252
[SwitchB-Vlan-interface500] quit
[SwitchB] vlan 600
[SwitchB-Vlan600] interface Vlan-interface600
[SwitchB-Vlan-interface600] ip address 1.1.5.5 255.255.255.252
[SwitchB-Vlan-interface600] quit
```

#### # Configure IP addresses for interfaces on Switch C.

```
<SwitchC> system-view
[SwitchC] vlan 600
[SwitchC-Vlan600] interface Vlan-interface600
[SwitchC-Vlan-interface600] ip address 1.1.5.6 255.255.255.252
[SwitchC-Vlan-interface600] quit
[SwitchC] vlan 900
[SwitchC-Vlan900] interface Vlan-interface900
[SwitchC-Vlan-interface900] ip address 1.1.3.1 255.255.255.0
[SwitchC-Vlan-interface900] quit
```

## 2. Configure static routes:

#### # Configure a default route on Switch A.

```
<SwitchA> system-view
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
```

#### # Configure two static routes on Switch B.

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.4.1
[SwitchB] ip route-static 1.1.3.0 255.255.255.0 1.1.5.6
```

#### # Configure a default route on Switch C.

```
<SwitchC> system-view
[SwitchC] ip route-static 0.0.0.0 0.0.0.0 1.1.5.5
```

## 3. Configure the default gateways of Host A, Host B, and Host C as 1.1.2.3, 1.1.6.1, and 1.1.3.1. (Details not shown.)

## Verifying the configuration

Use the **ping** command on the hosts to test the reachability. All hosts can reach one another.

## Configuration files

- Switch A:

```
#
vlan 300
#
vlan 500
#
interface Vlan-interface300
 ip address 1.1.2.3 255.255.255.0
#
interface Vlan-interface500
 ip address 1.1.4.1 255.255.255.252
#
ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
#
```
- Switch B:

```
#
vlan 100
#
vlan 500
#
vlan 600
#
interface Vlan-interface100
 ip address 1.1.6.1 255.255.255.0
#
interface Vlan-interface500
 ip address 1.1.4.2 255.255.255.252
#
interface Vlan-interface600
 ip address 1.1.5.5 255.255.255.252
#
ip route-static 1.1.2.0 255.255.255.0 1.1.4.1
ip route-static 1.1.3.0 255.255.255.0 1.1.5.6
#
```
- Switch C:

```
#
vlan 600
#
vlan 900
```

```
#
interface Vlan-interface600
 ip address 1.1.5.6 255.255.255.252
#
interface Vlan-interface900
 ip address 1.1.3.1 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.5.5
#
```

## Example: Configuring static routing-Track-NQA collaboration

### Applicable product matrix

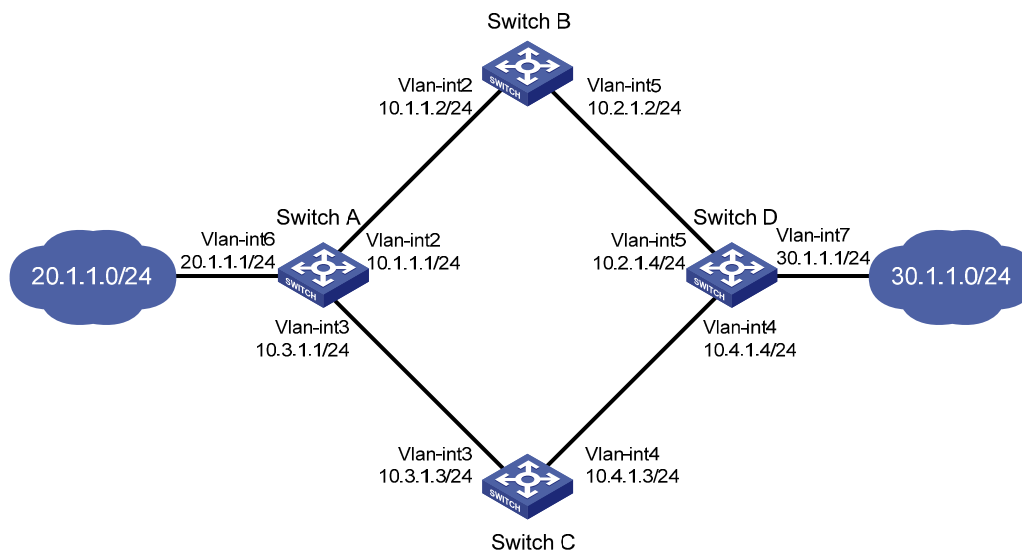
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

### Network requirements

As shown in [Figure 222](#):

- Configure static routes on these switches so that the two networks can communicate with each other.
- Configure static routing-Track-NQA collaboration to enable fast link switchover when the primary route fails and to improve network availability.

Figure 222 Network diagram



## Configuration restrictions and guidelines

When you configure static routing-Track-NQA collaboration, follow these restrictions and guidelines:

- When you configure an ICMP-echo operation to test the connectivity of a path, you must specify the next hop to define the path.
- You cannot enter the operation view of a scheduled NQA operation. To modify the operation, first use the **undo nqa schedule** command to stop the operation.

## Configuration procedures

1. Configure the IP address for interfaces, as shown in Figure 222. (Details not shown.)
2. Configure Switch A:
  - # Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.1.1.2 and the default priority 60. This static route is associated with track entry 1.

```
<SwitchA> system-view
[SwitchA] ip route-static 30.1.1.0 24 10.1.1.2 track 1
```
- # Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.3.1.3 and the priority 80.

```
[SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
```

- # Configure a static route to 10.2.1.4, with the address of the next hop as 10.1.1.2.

```
[SwitchA] ip route-static 10.2.1.4 24 10.1.1.2
```

- # Create an NQA test group with the administrator **admin** and the operation tag **test**.

```
[SwitchA] nqa entry admin test
```

- # Configure the test type as ICMP-echo.

```
[SwitchA-nqa-admin-test] type icmp-echo
Configure the destination address of the test as 10.2.1.4 and the next hop address as 10.1.1.2.
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.2.1.4
[SwitchA-nqa-admin-test-icmp-echo] next-hop 10.1.1.2
Configure the test frequency as 100 milliseconds.
[SwitchA-nqa-admin-test-icmp-echo] frequency 100
Configure reaction entry 1, and specify that five consecutive probe failures trigger the Track
module.
[SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail
threshold-type consecutive 5 action-type trigger-only
[SwitchA-nqa-admin-test-icmp-echo] quit
Start the NQA test.
[SwitchA] nqa schedule admin test start-time now lifetime forever
Configure track entry 1, and associate it with reaction entry 1 of the NQA test group (with the
administrator admin, and the operation tag test).
[SwitchA] track 1 nqa entry admin test reaction 1
```

### 3. Configure Switch B:

```
Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.2.1.4.
<SwitchB> system-view
[SwitchB] ip route-static 30.1.1.0 24 10.2.1.4
Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.1.1.1.
[SwitchB] ip route-static 20.1.1.0 24 10.1.1.1
```

### 4. Configure Switch C:

```
Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.4.1.4.
<SwitchC> system-view
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.4
Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.3.1.1.
[SwitchC] ip route-static 20.1.1.0 24 10.3.1.1
```

### 5. Configure Switch D:

```
Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.2.1.2 and the
default priority 60. This static route is associated with track entry 1.
<SwitchD> system-view
[SwitchD] ip route-static 20.1.1.0 24 10.2.1.2 track 1
Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.4.1.3 and the
priority 80.
[SwitchD] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
Configure a static route to 10.1.1.1, with the address of the next hop as 10.2.1.2.
[SwitchD] ip route-static 10.1.1.1 24 10.2.1.2
Create an NQA test group with the administrator admin and the operation tag test.
[SwitchD] nqa entry admin test
Configure the test type as ICMP-echo.
```

```

[SwitchD-nqa-admin-test] type icmp-echo
Configure the destination address of the test as 10.1.1.1 and the next hop address as 10.2.1.2.
[SwitchD-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
[SwitchD-nqa-admin-test-icmp-echo] next-hop 10.2.1.2
Configure the test frequency as 100 milliseconds.
[SwitchD-nqa-admin-test-icmp-echo] frequency 100
Configure reaction entry 1, and specify that five consecutive probe failures trigger the Track
module.
[SwitchD-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail
threshold-type consecutive 5 action-type trigger-only
[SwitchD-nqa-admin-test-icmp-echo] quit
Start the NQA test.
[SwitchD] nqa schedule admin test start-time now lifetime forever
Configure track entry 1, and associate it with reaction entry 1 of the NQA test group (with the
administrator admin, and the operation tag test).
[SwitchD] track 1 nqa entry admin test reaction 1

```

## Verifying the configuration

# Display information about the track entry on Switch A.

```

[SwitchA] display track all
Track ID: 1
 Status: Positive
 Notification delay: Positive 0, Negative 0 (in seconds)
 Reference object:
 NQA entry: admin test
 Reaction: 1

```

# Display the routing table of Switch A.

```

[SwitchA] display ip routing-table
Routing Tables: Public
 Destinations : 10 Routes : 10
Destination/Mask Proto Pre Cost NextHop Interface
10.1.1.0/24 Direct 0 0 10.1.1.1 Vlan2
10.1.1.1/32 Direct 0 0 127.0.0.1 InLoop0
10.2.1.0/24 Static 60 0 10.1.1.2 Vlan2
10.3.1.0/24 Direct 0 0 10.3.1.1 Vlan3
10.3.1.1/32 Direct 0 0 127.0.0.1 InLoop0
20.1.1.0/24 Direct 0 0 20.1.1.1 Vlan6
20.1.1.1/32 Direct 0 0 127.0.0.1 InLoop0
30.1.1.0/24 Static 60 0 10.1.1.2 Vlan2
127.0.0.0/8 Direct 0 0 127.0.0.1 InLoop0
127.0.0.1/32 Direct 0 0 127.0.0.1 InLoop0

```

The output shows the following NQA test results:

- The primary route is available (the status of the track entry is Positive).

- Switch A forwards packets to 30.1.1.0/24 through Switch B.

# Remove the IP address of interface VLAN-interface 2 on Switch B.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] shutdown
```

# Display information about the track entry on Switch A.

```
[SwitchA] display track all
Track ID: 1
 Status: Negative
 Notification delay: Positive 0, Negative 0 (in seconds)
 Reference object:
 NQA entry: admin test
 Reaction: 1
```

# Display the routing table of Switch A.

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

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	Direct	0	0	10.1.1.1	Vlan2
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.2.1.0/24	Static	60	0	10.1.1.2	Vlan2
10.3.1.0/24	Direct	0	0	10.3.1.1	Vlan3
10.3.1.1/32	Direct	0	0	127.0.0.1	InLoop0
20.1.1.0/24	Direct	0	0	20.1.1.1	Vlan6
20.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
30.1.1.0/24	Static	80	0	10.3.1.3	Vlan3
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

The output shows the following NQA test results:

- The primary route is unavailable (the status of the track entry is Negative).
- The backup static route takes effect.
- Switch A forwards packets to 30.1.1.0/24 through Switch C.

# When the primary route fails, the hosts in 20.1.1.0/24 can still communicate with the hosts in 30.1.1.0/24.

```
[SwitchA] ping -a 20.1.1.1 30.1.1.1
PING 30.1.1.1: 56 data bytes, press CTRL_C to break
 Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
 Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
 Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
 Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
 Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
--- 30.1.1.1 ping statistics ---
```



```
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/1/2 ms
```

# The output on Switch D is similar to that on Switch A. When the primary route fails, the hosts in 30.1.1.0/24 can still communicate with the hosts in 20.1.1.0/24.

```
[SwitchD] ping -a 30.1.1.1 20.1.1.1
PING 20.1.1.1: 56 data bytes, press CTRL_C to break
 Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
 Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
 Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
 Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
 Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
--- 20.1.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/2 ms
```

## Configuration files

- Switch A:

```
#
nqa entry admin test
 type icmp-echo
 destination ip 10.2.1.4
 frequency 100
 next-hop 10.1.1.2
 reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
 trigger-only
#
ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
ip route-static 30.1.1.0 255.255.255.0 10.1.1.2 track 1
ip route-static 30.1.1.0 255.255.255.0 10.3.1.3 preference 80
#
track 1 nqa entry admin test reaction 1
#
nqa schedule admin test start-time now lifetime forever
#
```

- Switch B:

```
ip route-static 20.1.1.0 255.255.255.0 10.1.1.1
ip route-static 30.1.1.0 255.255.255.0 10.2.1.4
```

- Switch C:

```
ip route-static 20.1.1.0 255.255.255.0 10.3.1.1
ip route-static 30.1.1.0 255.255.255.0 10.4.1.4
```

- Switch D:

```

#
nqa entry admin test
 type icmp-echo
 destination ip 10.1.1.1
 frequency 100
 next-hop 10.2.1.2
 reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
trigger-only
#
ip route-static 10.1.1.0 255.255.255.0 10.2.1.2
ip route-static 20.1.1.0 255.255.255.0 10.2.1.2 track 1
ip route-static 20.1.1.0 255.255.255.0 10.4.1.3 preference 80
#
track 1 nqa entry admin test reaction 1
#
nqa schedule admin test start-time now lifetime forever
#

```

## Example: Configuring static routing-Track-BFD collaboration

### Applicable product matrix

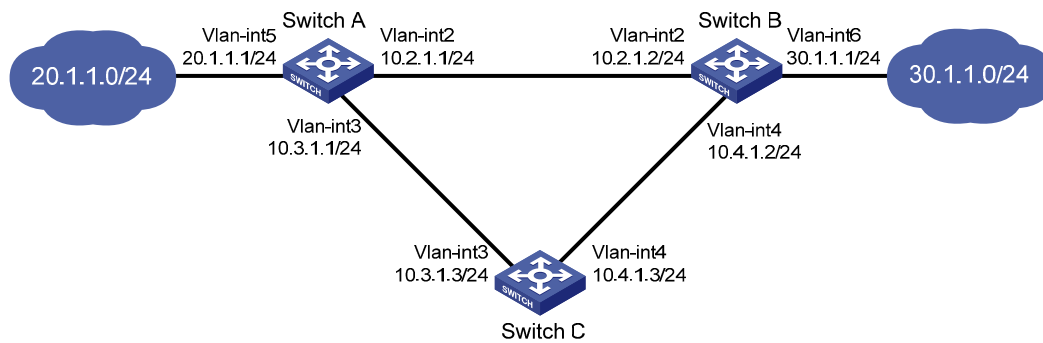
Product series	Software version
HP 5500 EI	Release 2220

### Network requirements

As shown in [Figure 223](#):

- Configure static routes on these switches so that the two networks can communicate with each other.
- Configure static routing-Track-BFD collaboration to enable fast link switchover when the primary route fails and to improve network availability.

Figure 223 Network diagram



## Configuration restrictions and guidelines

The source IP address of BFD echo packets cannot be on the same network segment as any local interface's IP address. Otherwise, a large number of ICMP redirect packets might be sent from the peer, resulting in link congestion.

## Configuration procedures

1. Configure the IP address for interfaces, as shown in Figure 223. (Details not shown.)
2. Configure Switch A:
  - # Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.2.1.2 and the default priority 60. This static route is associated with track entry 1.

```
<SwitchA> system-view
[SwitchA] ip route-static 30.1.1.0 24 10.2.1.2 track 1
```
- # Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.3.1.3 and the priority 80.

```
[SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
```

- # Configure the source address of BFD echo packets as 10.10.10.10.

```
[SwitchA] bfd echo-source-ip 10.10.10.10
```

- # Configure track entry 1, and associate it with the BFD session. Check whether Switch A can be interoperated with the next hop (Switch B) of the static route.

```
[SwitchA] track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.2 local ip 10.2.1.1
```

3. Configure Switch B:
  - # Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.2.1.1 and the default priority 60. This static route is associated with track entry 1.

```
<SwitchB> system-view
[SwitchB] ip route-static 20.1.1.0 24 10.2.1.1 track 1
```

# Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.4.1.3 and the priority 80.

```
[SwitchB] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

# Configure the source address of BFD echo packets as 1.1.1.1.

```
[SwitchB] bfd echo-source-ip 1.1.1.1
```

# Configure track entry 1 that is associated with the BFD session to check whether Switch B can communicate with the next hop (Switch A) of the static route.

```
[SwitchB] track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.1 local ip 10.2.1.2
```

#### 4. Configure Switch C:

# Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.4.1.2.

```
<SwitchC> system-view
```

```
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.2
```

# Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.3.1.1.

```
[SwitchC] ip route-static 20.1.1.0 24 10.3.1.1
```

## Verifying the configuration

# Display information about the track entry on Switch A.

```
[SwitchA] display track all
```

```
Track ID: 1
```

```
Status: Positive
```

```
Notification delay: Positive 0, Negative 0 (in seconds)
```

```
Reference object:
```

```
BFD Session:
```

```
Packet type: Echo
```

```
Interface : Vlan-interface2
```

```
Remote IP : 10.2.1.2
```

```
Local IP : 10.2.1.1
```

# Display the routing table of Switch A.

```
[SwitchA] display ip routing-table
```

```
Routing Tables: Public
```

```
Destinations : 9 Routes : 9
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.2.1.0/24	Direct	0	0	10.2.1.1	Vlan2
10.2.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.3.1.0/24	Direct	0	0	10.3.1.1	Vlan3
10.3.1.1/32	Direct	0	0	127.0.0.1	InLoop0
20.1.1.0/24	Direct	0	0	20.1.1.1	Vlan5
20.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
30.1.1.0/24	Static	60	0	10.2.1.2	Vlan2
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

The output shows the following BFD detection results:

- The next hop 10.2.1.2 is reachable (the status of the track entry is Positive).
- The primary static route takes effect.
- Switch A forwards packets to 30.1.1.0/24 through Switch B.

# Remove the IP address of interface VLAN-interface 2 on Switch B.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] shutdown
```

# Display information about the track entry on Switch A.

```
[SwitchA] display track all
Track ID: 1
 Status: Negative
 Notification delay: Positive 0, Negative 0 (in seconds)
 Reference object:
 BFD Session:
 Packet type: Echo
 Interface : Vlan-interface2
 Remote IP : 10.2.1.2
 Local IP : 10.2.1.1
```

# Display the routing table of Switch A.

```
[SwitchA] display ip routing-table
Routing Tables: Public
 Destinations : 4 Routes : 4
Destination/Mask Proto Pre Cost NextHop Interface
10.2.1.0/24 Direct 0 0 10.2.1.1 Vlan2
10.2.1.1/32 Direct 0 0 127.0.0.1 InLoop0
10.3.1.0/24 Direct 0 0 10.3.1.1 Vlan3
10.3.1.1/32 Direct 0 0 127.0.0.1 InLoop0
20.1.1.0/24 Direct 0 0 20.1.1.1 Vlan5
20.1.1.1/32 Direct 0 0 127.0.0.1 InLoop0
30.1.1.0/24 Static 80 0 10.3.1.3 Vlan3
127.0.0.0/8 Direct 0 0 127.0.0.1 InLoop0
127.0.0.1/32 Direct 0 0 127.0.0.1 InLoop0
```

The output shows the following BFD detection results:

- The next hop 10.2.1.2 is unreachable (the status of the track entry is Negative).
- The backup static route takes effect.
- Switch A forwards packets to 30.1.1.0/24 through Switch C and Switch B.

# When the primary route fails, the hosts in 20.1.1.0/24 can still communicate with the hosts in 30.1.1.0/24.

```
[SwitchA] ping -a 20.1.1.1 30.1.1.1
PING 30.1.1.1: 56 data bytes, press CTRL_C to break
 Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
 Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
 Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
```

```

Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
--- 30.1.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/2 ms

```

# The output on Switch B is similar to that on Switch A. When the primary route fails, the hosts in 30.1.1.0/24 can still communicate with the hosts in 20.1.1.0/24.

```

[SwitchB] ping -a 30.1.1.1 20.1.1.1
PING 20.1.1.1: 56 data bytes, press CTRL_C to break
Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
--- 20.1.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/2 ms

```

## Configuration files

- Switch A:

```

#
bfd echo-source-ip 10.10.10.10
#
ip route-static 30.1.1.0 24 10.2.1.2 track 1
ip route-static 30.1.1.0 24 10.3.1.3 preference 80
#
track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.2 local ip 10.2.1.1
#

```
- Switch B:

```

#
bfd echo-source-ip 1.1.1.1
#
ip route-static 30.1.1.0 24 10.2.1.2 track 1
ip route-static 20.1.1.0 24 10.4.1.3 preference 80
#
track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.1 local ip 10.2.1.2
#

```
- Switch C:

```

#
ip route-static 20.1.1.0 24 10.3.1.1
ip route-static 30.1.1.0 24 10.4.1.2

```

#

# Tunnel configuration examples

This chapter provides tunnel configuration examples.

## Example: Configuring an IPv6 over IPv4 manual tunnel

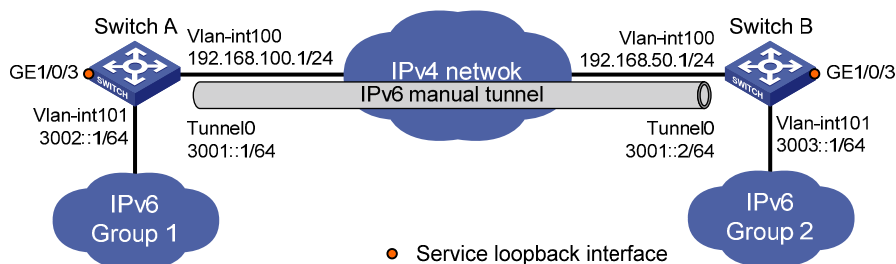
### Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

### Network requirements

As shown in [Figure 224](#), Switch A and Switch B can reach each other. Configure an IPv6 over IPv4 manual tunnel between Switch A and Switch B so the two IPv6 networks can reach each other over the IPv4 network.

**Figure 224 Network diagram**



### Configuration restrictions and guidelines

Before you configure a tunnel interface, perform the following tasks:

- Create a tunnel-type service loopback group.
- Add unused Layer 2 Ethernet interfaces into the group.



# Configuration procedures

## Configuring Switch A

# Enable IPv6.

```
<SwitchA> system-view
[SwitchA] ipv6
```

# Specify an IPv4 address for VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 192.168.100.1 255.255.255.0
[SwitchA-Vlan-interface100] quit
```

# Specify an IPv6 address for VLAN-interface 101.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ipv6 address 3002::1 64
[SwitchA-Vlan-interface101] quit
```

# Configure an IPv6 over IPv4 manual tunnel.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ipv6 address 3001::1/64
[SwitchA-Tunnel0] source vlan-interface 100
[SwitchA-Tunnel0] destination 192.168.50.1
[SwitchA-Tunnel0] tunnel-protocol ipv6-ipv4
[SwitchA-Tunnel0] quit
```

# Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchA] service-loopback group 1 type tunnel
```

# Assign GigabitEthernet 1/0/3 to service loopback group 1, and disable STP, NDP, and LLDP on the interface.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] undo stp enable
[SwitchA-GigabitEthernet1/0/3] undo ndp enable
[SwitchA-GigabitEthernet1/0/3] undo lldp enable
[SwitchA-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-GigabitEthernet1/0/3] quit
```

# Apply service loopback group 1 to the tunnel interface.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] service-loopback-group 1
[SwitchA-Tunnel0] quit
```

# Configure a static route to IPv6 network Group 2 through the tunnel interface.

```
[SwitchA] ipv6 route-static 3003:: 64 tunnel 0
```

## Configuring Switch B

# Enable IPv6.

```
<SwitchB> system-view
[SwitchB] ipv6
```

# Specify an IPv4 address for VLAN-interface 100.

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 192.168.50.1 255.255.255.0
[SwitchB-Vlan-interface100] quit
```

# Specify an IPv6 address for VLAN-interface 101.

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ipv6 address 3003::1 64
[SwitchB-Vlan-interface101] quit
```

# Configure an IPv6 over IPv4 manual tunnel.

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] ipv6 address 3001::2/64
[SwitchB-Tunnel0] source vlan-interface 100
[SwitchB-Tunnel0] destination 192.168.100.1
[SwitchB-Tunnel0] tunnel-protocol ipv6-ipv4
[SwitchB-Tunnel0] quit
```

# Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchB] service-loopback group 1 type tunnel
```

# Assign GigabitEthernet 1/0/3 to service loopback group 1, and disable STP, NDP, and LLDP on the interface.

```
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] undo stp enable
[SwitchB-GigabitEthernet1/0/3] undo ndp enable
[SwitchB-GigabitEthernet1/0/3] undo lldp enable
[SwitchB-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-GigabitEthernet1/0/3] quit
```

# Apply service loopback group 1 to the tunnel interface.

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] service-loopback-group 1
[SwitchB-Tunnel0] quit
```

# Configure a static route to IPv6 network Group 1 through the tunnel interface.

```
[SwitchB] ipv6 route-static 3002:: 64 tunnel 0
```

## Verifying the configuration

# Display the status of the tunnel interface on Switch A.

```
[SwitchA] display ipv6 interface tunnel 0 verbose
Tunnel0 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::C0A8:6401
 Global unicast address(es):
 3001::1, subnet is 3001::/64
 Joined group address(es):
 FF02::1:FF00:0
 FF02::1:FF00:1
```

```

 FF02::1:FFA8:6401
 FF02::2
 FF02::1
MTU is 1480 bytes
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
 InReceives: 55
...
Display the status of the tunnel interface on Switch B.
[SwitchB] display ipv6 interface tunnel 0 verbose
Tunnel0 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::C0A8:3201
Global unicast address(es):
 3001::2, subnet is 3001::/64
Joined group address(es):
 FF02::1:FF00:0
 FF02::1:FF00:1
 FF02::1:FFA8:3201
 FF02::2
 FF02::1
MTU is 1480 bytes
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
 InReceives: 55
...

```

# Ping the IPv6 address of the peer interface VLAN-interface 101 from Switch A. The ping operation succeeds.

```

[SwitchA] ping ipv6 3003::1
PING 3003::1 : 56 data bytes, press CTRL_C to break
 Reply from 3003::1
 bytes=56 Sequence=1 hop limit=64 time = 1 ms
 Reply from 3003::1
 bytes=56 Sequence=2 hop limit=64 time = 1 ms
 Reply from 3003::1
 bytes=56 Sequence=3 hop limit=64 time = 1 ms
 Reply from 3003::1
 bytes=56 Sequence=4 hop limit=64 time = 1 ms
 Reply from 3003::1
 bytes=56 Sequence=5 hop limit=64 time = 1 ms

--- 3003::1 ping statistics ---
 5 packet(s) transmitted

```

```
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/1/1 ms
```

## Configuration files

- Switch A:

```
#
ipv6
#
service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
ip address 192.168.100.1 255.255.255.0
#
interface Vlan-interface101
ipv6 address 3002::1/64
#
interface GigabitEthernet1/0/3
port link-mode bridge
stp disable
undo ndp enable
undo lldp enable
port service-loopback group 1
#
interface Tunnel0
ipv6 address 3001::1/64
tunnel-protocol ipv6-ipv4
source Vlan-interface100
destination 192.168.50.1
service-loopback-group 1
#
ipv6 route-static 3003:: 64 Tunnel0
#
```

- Switch B:

```
#
ipv6
#
service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
ip address 192.168.50.1 255.255.255.0
#
```

```

interface Vlan-interface101
 ipv6 address 3003::1/64
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 stp disable
 undo ndp enable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ipv6 address 3001::2/64
 tunnel-protocol ipv6-ipv4
 source Vlan-interface100
 destination 192.168.100.1
 service-loopback-group 1
#
 ipv6 route-static 3002:: 64 Tunnel0
#

```

## Example: Configuring a 6to4 tunnel

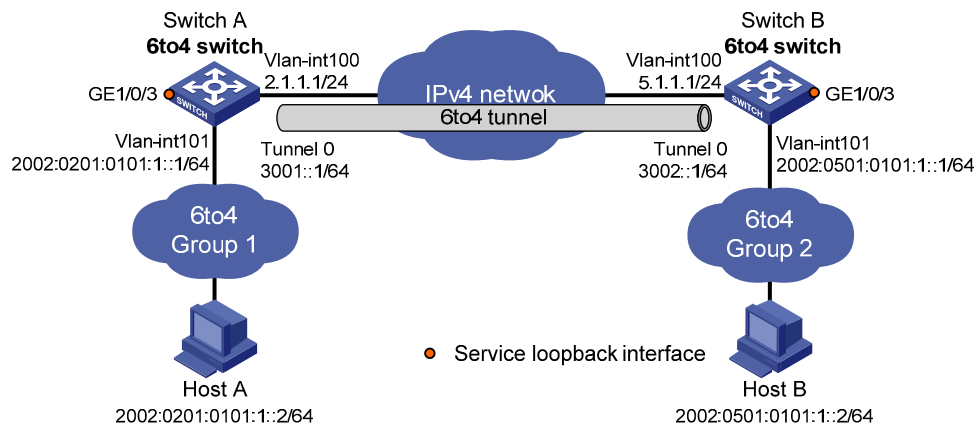
### Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

### Network requirements

As shown in [Figure 225](#), Switch A and Switch B can reach each other. Configure a 6to4 tunnel between the 6to4 switches Switch A and Switch B so Host A and Host B can reach each other over the IPv4 network.

Figure 225 Network diagram



## Configuration restrictions and guidelines

Before you configure a tunnel interface, perform the following tasks:

- Create a tunnel-type service loopback group.
- Add unused Layer 2 Ethernet interfaces into the group.

## Configuration procedures

### Configuring Switch A

# Enable IPv6.

```
<SwitchA> system-view
[SwitchA] ipv6
```

# Specify an IPv4 address for VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 2.1.1.1 24
[SwitchA-Vlan-interface100] quit
```

# Specify an IPv6 address for VLAN-interface 101.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ipv6 address 2002:0201:0101:1::1/64
[SwitchA-Vlan-interface101] quit
```

# Configure a 6to4 tunnel.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ipv6 address 3001::1/64
[SwitchA-Tunnel0] source vlan-interface 100
[SwitchA-Tunnel0] tunnel-protocol ipv6-ipv4 6to4
[SwitchA-Tunnel0] quit
```

# Create service loopback group 1, and specify its service type as **tunnel**.

```
[SwitchA] service-loopback group 1 type tunnel

Assign GigabitEthernet 1/0/3 to service loopback group 1, and disable STP, NDP, and LLDP on the interface.

[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] undo stp enable
[SwitchA-GigabitEthernet1/0/3] undo ndp enable
[SwitchA-GigabitEthernet1/0/3] undo lldp enable
[SwitchA-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-GigabitEthernet1/0/3] quit

Apply service loopback group 1 to the tunnel interface.

[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] service-loopback-group 1
[SwitchA-Tunnel0] quit

Configure a static route to 2002::/16 through the tunnel interface.

[SwitchA] ipv6 route-static 2002:: 16 tunnel 0
```

## Configuring Switch B

```
Enable IPv6.

<SwitchB> system-view
[SwitchB] ipv6

Specify an IPv4 address for VLAN-interface 100.

[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 5.1.1.1 24
[SwitchB-Vlan-interface100] quit

Specify an IPv6 address for VLAN-interface 101.

[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ipv6 address 2002:0501:0101:1::1/64
[SwitchB-Vlan-interface101] quit

Configure a 6to4 tunnel.

[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] ipv6 address 3002::1/64
[SwitchB-Tunnel0] source vlan-interface 100
[SwitchB-Tunnel0] tunnel-protocol ipv6-ipv4 6to4
[SwitchB-Tunnel0] quit

Create service loopback group 1, and specify its service type as tunnel.

[SwitchB] service-loopback group 1 type tunnel

Assign GigabitEthernet 1/0/3 to service loopback group 1, and disable STP, NDP, and LLDP on the interface.

[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] undo stp enable
[SwitchB-GigabitEthernet1/0/3] undo ndp enable
[SwitchB-GigabitEthernet1/0/3] undo lldp enable
[SwitchB-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-GigabitEthernet1/0/3] quit
```

```
Apply service loopback group 1 to the tunnel interface.
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] service-loopback-group 1
[SwitchB-Tunnel0] quit

Configure a static route to 2002::/16 through the tunnel interface.
[SwitchB] ipv6 route-static 2002:: 16 tunnel 0
```

## Verifying the configuration

```
Ping either host from the other, and 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:

```
#
 ipv6
#
 service-loopback group 1 type tunnel
#
vlan 2
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 2.1.1.1 255.255.255.0
#
interface Vlan-interface101
 ipv6 address 2002:201:101:1::1/64
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 stp disable
```



```

undo ndp enable
undo lldp enable
port service-loopback group 1
#
interface Tunnel0
 ipv6 address 3001::1/64
 tunnel-protocol ipv6-ipv4 6to4
 source Vlan-interface100
 service-loopback-group 1
#
 ipv6 route-static 2002:: 16 Tunnel0
#

```

- Switch B:

```

#
 ipv6
#
 service-loopback group 1 type tunnel
#
vlan 2
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 5.1.1.1 255.255.255.0
#
interface Vlan-interface101
 ipv6 address 2002:0501:0101:1::1/64
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 stp disable
 undo ndp enable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ipv6 address 3002::1/64
 tunnel-protocol ipv6-ipv4 6to4
 source Vlan-interface100
 service-loopback-group 1
#
 ipv6 route-static 2002:: 16 Tunnel0
#

```

# Example: Configuring an ISATAP tunnel

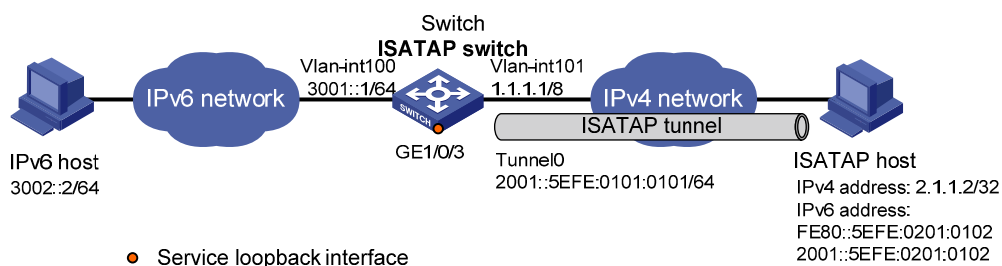
## Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

## Network requirements

As shown in [Figure 226](#), configure an ISATAP tunnel between the ISATAP switch and the ISATAP host so the ISATAP host in the IPv4 network can access the IPv6 network.

**Figure 226 Network diagram**



## Configuration restrictions and guidelines

Before you configure a tunnel interface, perform the following tasks:

- Create a tunnel-type service loopback group.
- Add unused Layer 2 Ethernet interfaces into the group.

## Configuration procedures

### Configuring the ISATAP switch

```
Enable IPv6.
<Switch> system-view
[Switch] ipv6

Specify IP addresses for interfaces.
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 3001::1/64
[Switch-Vlan-interface100] quit
[Switch] interface vlan-interface 101
```

```
[Switch-Vlan-interface101] ip address 1.1.1.1 255.0.0.0
[Switch-Vlan-interface101] quit
```

# Configure an ISATAP tunnel.

```
[Switch] interface tunnel 0
[Switch-Tunnel0] ipv6 address 2001::/64 eui-64
[Switch-Tunnel0] source vlan-interface 101
[Switch-Tunnel0] tunnel-protocol ipv6-ipv4 isatap
```

# Disable RA suppression so that the ISATAP host can obtain the address prefix carried in the RA message advertised by the ISATAP switch.

```
[Switch-Tunnel0] undo ipv6 nd ra halt
[Switch-Tunnel0] quit
```

# Create service loopback group 1, and specify its service type as **tunnel**.

```
[Switch] service-loopback group 1 type tunnel
```

# Assign GigabitEthernet 1/0/3 to service loopback group 1, and disable STP, NDP, and LLDP on the interface.

```
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] undo stp enable
[Switch-GigabitEthernet1/0/3] undo ndp enable
[Switch-GigabitEthernet1/0/3] undo lldp enable
[Switch-GigabitEthernet1/0/3] port service-loopback group 1
[Switch-GigabitEthernet1/0/3] quit
```

# Apply service loopback group 1 to the tunnel interface.

```
[Switch] interface tunnel 0
[Switch-Tunnel0] service-loopback-group 1
[Switch-Tunnel0] quit
```

## Configuring the ISATAP host

Configurations on the ISATAP host vary with the operating systems. The following example is performed on Windows XP:

# Install IPv6.

```
C:\>ipv6 install
```

# 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 that an ISATAP tunnel has been established.

```

C:\>ping 2001::5efe:1.1.1.1

Pinging 2001::5efe:1.1.1.1 with 32 bytes of data:

Reply from 2001::5efe:1.1.1.1: time=1ms
Reply from 2001::5efe:1.1.1.1: time=1ms
Reply from 2001::5efe:1.1.1.1: time=1ms
Reply from 2001::5efe:1.1.1.1: time=1ms

Ping statistics for 2001::5efe:1.1.1.1:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 1ms, Average = 1ms

```

# 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

```
#
 ipv6
#
 service-loopback group 1 type tunnel
#
vlan 100 to 101
#
interface Vlan-interface100
 ipv6 address 3001::1/64
#
interface Vlan-interface101
 ip address 1.1.1.1 255.0.0.0
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 stp disable
 undo ndp enable
 undo lldp enable
 port service-loopback group 1
#
interface Tunnel0
 ipv6 address 2001::/64 eui-64
 undo ipv6 nd ra halt
 tunnel-protocol ipv6-ipv4 isatap
 source Vlan-interface101
 service-loopback-group 1
#
```

# URPF configuration examples

This chapter provides Unicast Reverse Path Forwarding (URPF) configuration examples.

## Example: Configuring URPF

### Applicable product matrix

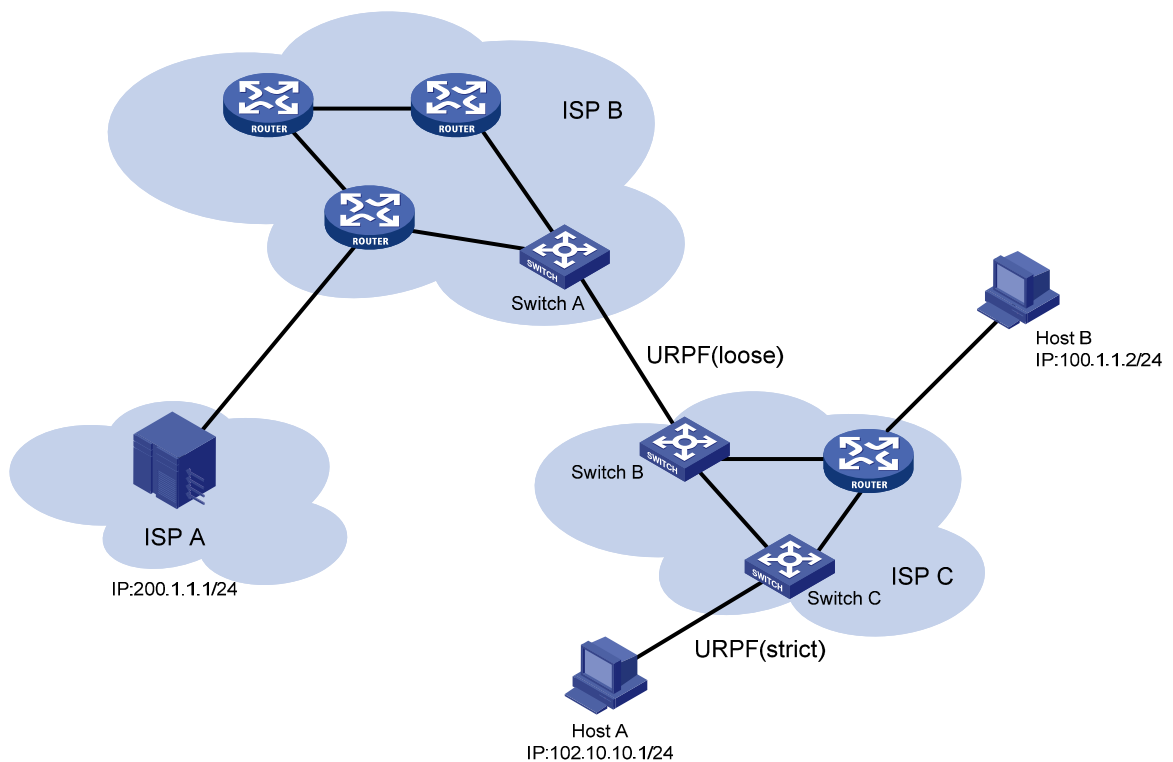
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

### Network requirements

As shown in [Figure 227](#):

- 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 227 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 5500 EI	Release 2220
HP 5500 SI	

### Network requirements

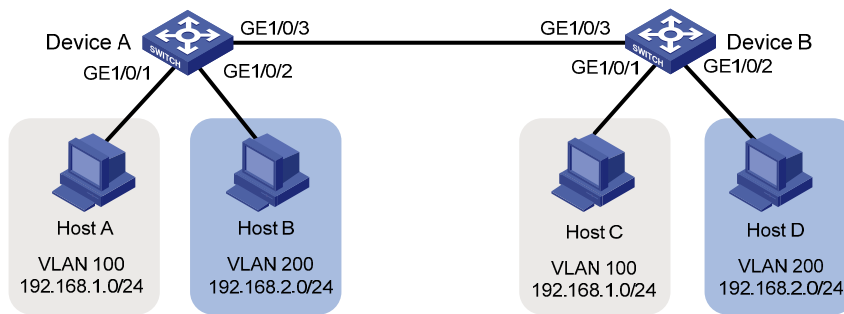
As shown in [Figure 228](#):

- 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 228 Network diagram



## Configuration procedures

### Configuring Device A

# Create VLAN 100, and assign the port GigabitEthernet 1/0/1 to VLAN 100.

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

# Create VLAN-interface 100, and configure its IP address as 192.168.1.1/24.

```
[DeviceA] interface Vlan-interface 100
[DeviceA-Vlan-interface100] ip address 192.168.1.1 24
[DeviceA-Vlan-interface100] quit
```

# Create VLAN 200, and assign the port GigabitEthernet 1/0/2 to VLAN 200.

```
[DeviceA] vlan 200
[DeviceA-vlan200] port gigabitethernet 1/0/2
[DeviceA-vlan200] quit
```

# Create VLAN-interface 200, and configure its IP address as 192.168.2.2/24.

```
[DeviceA] interface Vlan-interface 200
[DeviceA-Vlan-interface200] ip address 192.168.2.2 24
[DeviceA-Vlan-interface200] quit
```

# Configure the port GigabitEthernet 1/0/3 as a trunk port.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
```

# Assign the port GigabitEthernet 1/0/3 to VLANs 100 and 200.

```
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 100 200
```

# Remove the port GigabitEthernet 1/0/3 from VLAN 1.

```
[DeviceA-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/3] quit
```

### Configuring Device B

# Create VLAN 100, and assign the port GigabitEthernet 1/0/1 to VLAN 100.

```

<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] port gigabitethernet 1/0/1
[DeviceB-vlan100] quit

Create VLAN-interface 100, and configure its IP address as 192.168.1.2/24.
[DeviceB] interface Vlan-interface 100
[DeviceB-Vlan-interface100] ip address 192.168.1.2 24
[DeviceB-Vlan-interface100] quit

Create VLAN 200, and assign the port GigabitEthernet 1/0/2 to VLAN 200.
[DeviceB] vlan 200
[DeviceB-vlan200] port gigabitethernet 1/0/2
[DeviceB-vlan200] quit

Create VLAN-interface 200, and configure its IP address as 192.168.2.1/24.
[DeviceB] interface Vlan-interface 200
[DeviceB-Vlan-interface200] ip address 192.168.2.1 24
[DeviceB-Vlan-interface200] quit

Configure the port GigabitEthernet 1/0/3 as a trunk port.
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk

Assign the port GigabitEthernet 1/0/3 to VLANs 100 and 200.
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 100 200

Remove the port GigabitEthernet 1/0/3 from VLAN 1.
[DeviceB-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/3] quit

```

## Verifying the configuration

# Display information about VLAN 100 on Device A.

```

[DeviceA] display vlan 100
VLAN ID: 100
VLAN Type: static
Route Interface: configured
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Description: VLAN 0100
Name: VLAN 0100
Tagged Ports:
 GigabitEthernet1/0/3
Untagged Ports:
 GigabitEthernet1/0/1

```

# Display information about VLAN 200 on Device A.

```

[DeviceA] display vlan 200
VLAN ID: 200
VLAN Type: static

```

```
Route Interface: configured
IP Address: 192.168.2.2
Subnet Mask: 255.255.255.0
Description: VLAN 0200
Name: VLAN 0200
Tagged Ports:
 GigabitEthernet1/0/3
Untagged Ports:
 GigabitEthernet1/0/2
```

# Verify that Host A and Host B can ping each other. In the ARP table of Host A, an entry containing the IP address and MAC address of Host C exists. In the ARP table of Host C, an entry containing the IP address and MAC address of Host A exists.

# Verify that 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

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
```

- Device B:

```

#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#

```

## Example: Configuring dynamic MAC-based VLANs

### Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

This configuration example uses IMC PLAT 5.2 (E0401) and IMC UAM 5.2 (E0401).

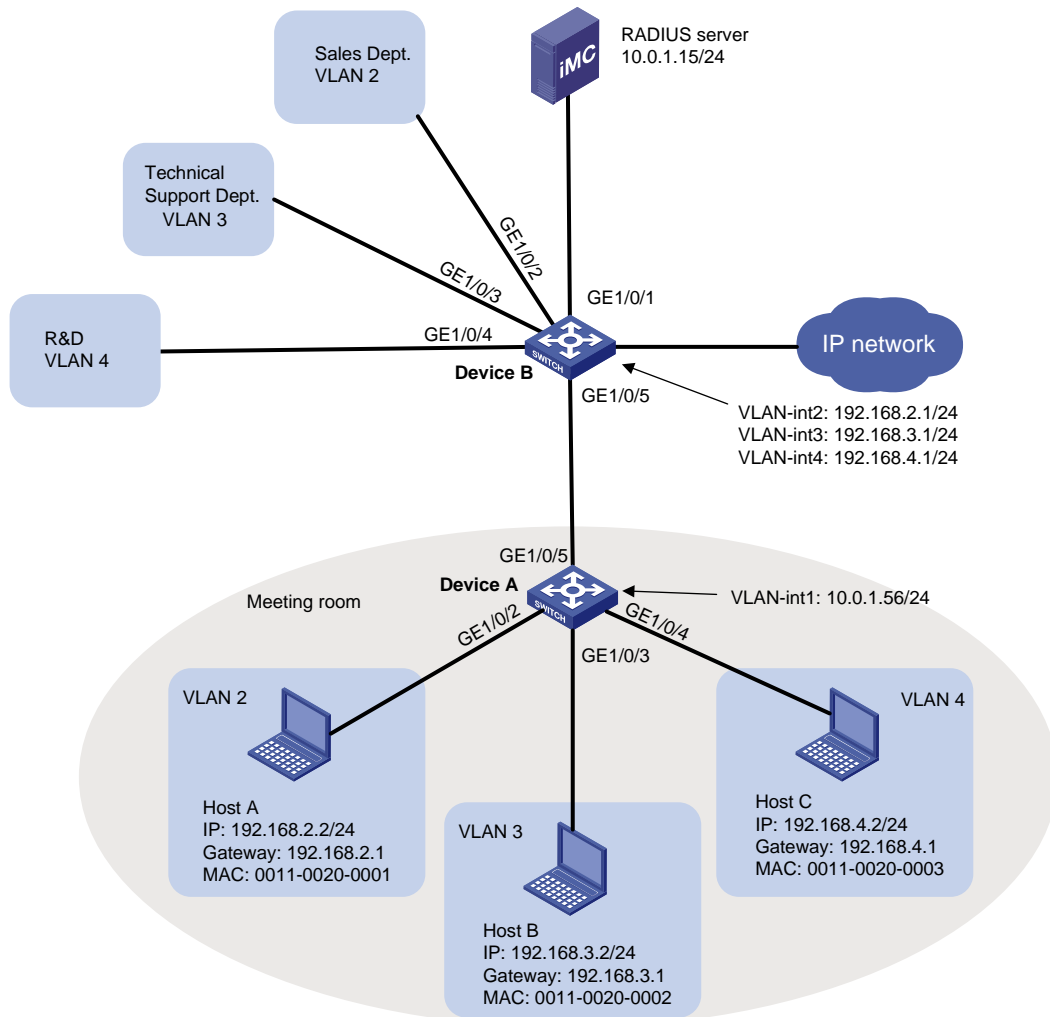
### Network requirements

As shown in [Figure 229](#), different departments belong to different VLANs.

Configure dynamic MAC-based VLANs to meet the following requirements:

- Users must pass 802.1X authentication to access the network.
- When the users of different departments access the IP network in the meeting room, the VLANs to which they belong do not change.

Figure 229 Network diagram



## Configuration restrictions and guidelines

When you configure dynamic MAC-based VLANs, follow these restrictions and guidelines:

- MAC-based VLANs are available only on hybrid ports.
- The MAC-based VLAN feature is typically configured on downlink ports of user access devices. Do not enable this feature together with link aggregation on downlink ports of user access devices.
- Do not configure a super VLAN as the VLAN of a MAC address-to-VLAN entry.

## Configuration procedures

### Configuring Device A

```
Create a RADIUS scheme named macvlan and enter RADIUS scheme view.
```

```
<DeviceA> system-view
```

```

[DeviceA] radius scheme macvlan
New Radius scheme

Configure the RADIUS server type of RADIUS scheme macvlan as extended.
[DeviceA-radius-macvlan] server-type extended

Specify the IP address of the authentication server and accounting server as 10.0.1.15.
[DeviceA-radius-macvlan] primary authentication 10.0.1.15
[DeviceA-radius-macvlan] primary accounting 10.0.1.15

Specify the shared key for secure authentication and accounting communication as expert. (Configure
the same shared key on the IMC server.)
[DeviceA-radius-macvlan] key authentication expert
[DeviceA-radius-macvlan] key accounting expert

Exclude the ISP domain name from the username that is sent to the RADIUS server.
[DeviceA-radius-macvlan] user-name-format without-domain
[DeviceA-radius-macvlan] quit

Use the default ISP domain system. Configure ISP domain system to use RADIUS scheme macvlan for
authentication, authorization, and accounting of all LAN users.
[DeviceA] domain system
[DeviceA-isp-system] authentication lan-access radius-scheme macvlan
[DeviceA-isp-system] authorization lan-access radius-scheme macvlan
[DeviceA-isp-system] accounting lan-access radius-scheme macvlan
[DeviceA-isp-system] quit

Enable 802.1X globally.
[DeviceA] undo port-security enable
[DeviceA] dot1x
802.1X is enabled globally.

Enable 802.1X on the ports GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet
1/0/4.
[DeviceA] dot1x interface gigabitethernet 1/0/2 to gigabitethernet 1/0/4
802.1x is enabled on port GigabitEthernet1/0/2.
802.1x is enabled on port GigabitEthernet1/0/3.
802.1x is enabled on port GigabitEthernet1/0/4.

Configure the port GigabitEthernet 1/0/2 as a hybrid port, and enable the MAC-based VLAN feature
on the port.
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type hybrid
[DeviceA-GigabitEthernet1/0/2] mac-vlan enable
[DeviceA-GigabitEthernet1/0/2] quit

Configure the port GigabitEthernet 1/0/3 as a hybrid port, and enable MAC-based VLAN feature on
the port.
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type hybrid
[DeviceA-GigabitEthernet1/0/3] mac-vlan enable
[DeviceA-GigabitEthernet1/0/3] quit

```

# Configure the port GigabitEthernet 1/0/4 as a hybrid port, and enable the MAC-based VLAN feature on the port.

```
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port link-type hybrid
[DeviceA-GigabitEthernet1/0/4] mac-vlan enable
[DeviceA-GigabitEthernet1/0/4] quit
```

# Configure the port GigabitEthernet 1/0/5 as a trunk port, and assign the port to VLAN 2, VLAN 3, and VLAN 4.

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port link-type trunk
[DeviceA-GigabitEthernet1/0/5] port trunk permit vlan 2 to 4
[DeviceA-GigabitEthernet1/0/5] quit
```

# Create VLAN-interface 1 and assign the IP address **10.0.1.56** to VLAN-interface 1. Device A uses this IP address to communicate with the RADIUS server.

```
[DeviceA] interface vlan-interface 1
[DeviceA-Vlan-interface1] ip address 10.0.1.56 24
[DeviceA-Vlan-interface1] quit
```

## Configuring Device B

# Assign the ports GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to VLAN 2, VLAN 3, and VLAN 4, respectively.

```
[DeviceB] vlan 2
[DeviceB-vlan2] port gigabitethernet 1/0/2
[DeviceB-vlan2] vlan 3
[DeviceB-vlan3] port gigabitethernet 1/0/3
[DeviceB-vlan3] vlan 4
[DeviceB-vlan4] port gigabitethernet 1/0/4
[DeviceB-vlan4] quit
```

# Create VLAN interfaces for VLAN 2 through VLAN 4 for inter-VLAN Layer 3 communication, and assign IP addresses to these VLAN interfaces, as shown in [Figure 229](#).

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ip address 192.168.2.1 24
[DeviceB-Vlan-interface2] interface vlan-interface 3
[DeviceB-Vlan-interface3] ip address 192.168.3.1 24
[DeviceB-Vlan-interface3] interface vlan-interface 4
[DeviceB-Vlan-interface4] ip address 192.168.4.1 24
[DeviceB-Vlan-interface4] quit
```

# Configure the port GigabitEthernet 1/0/5 as a trunk port, and assign the port to VLAN 2, VLAN 3, and VLAN 4.

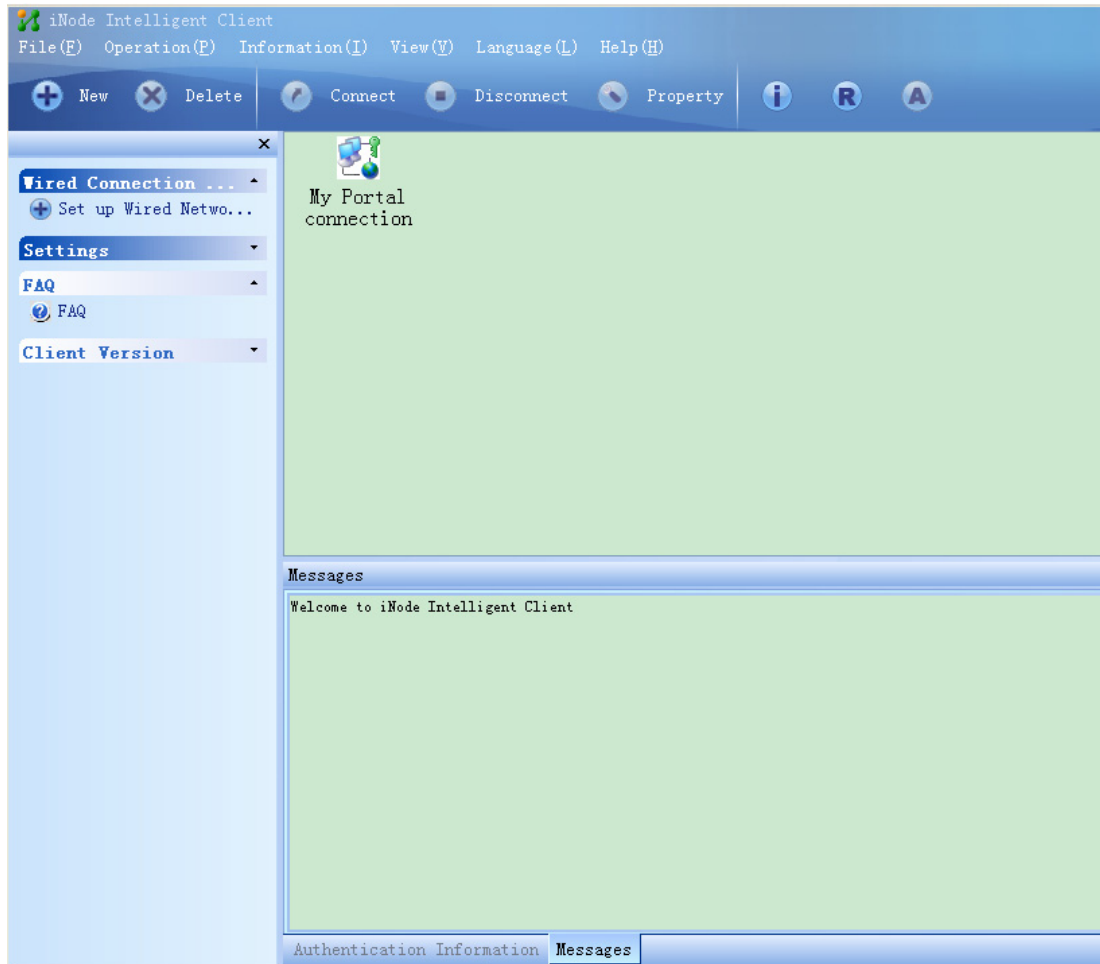
```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port link-type trunk
[DeviceA-GigabitEthernet1/0/5] port trunk permit vlan 2 to 4
[DeviceA-GigabitEthernet1/0/5] quit
```



## Configuring Host A

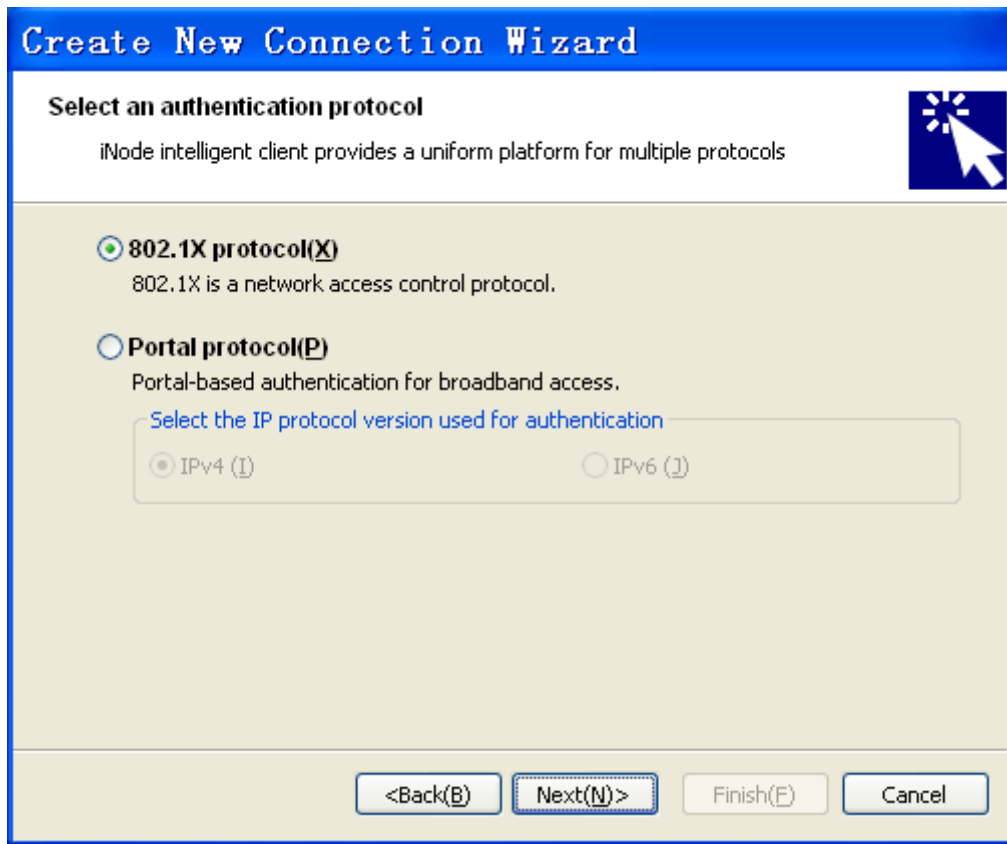
1. Configure the IP address of Host A as 192.168.2.2 with the subnet mask 255.255.255.0 and the default gateway 192.168.2.1/24. You can also use a DHCP server to assign an IP address on the subnet 192.168.2.1/24 to the host.
2. Install the HP iNode client software.
3. Open the iNode client as shown in Figure 230.

Figure 230 Opening iNode client



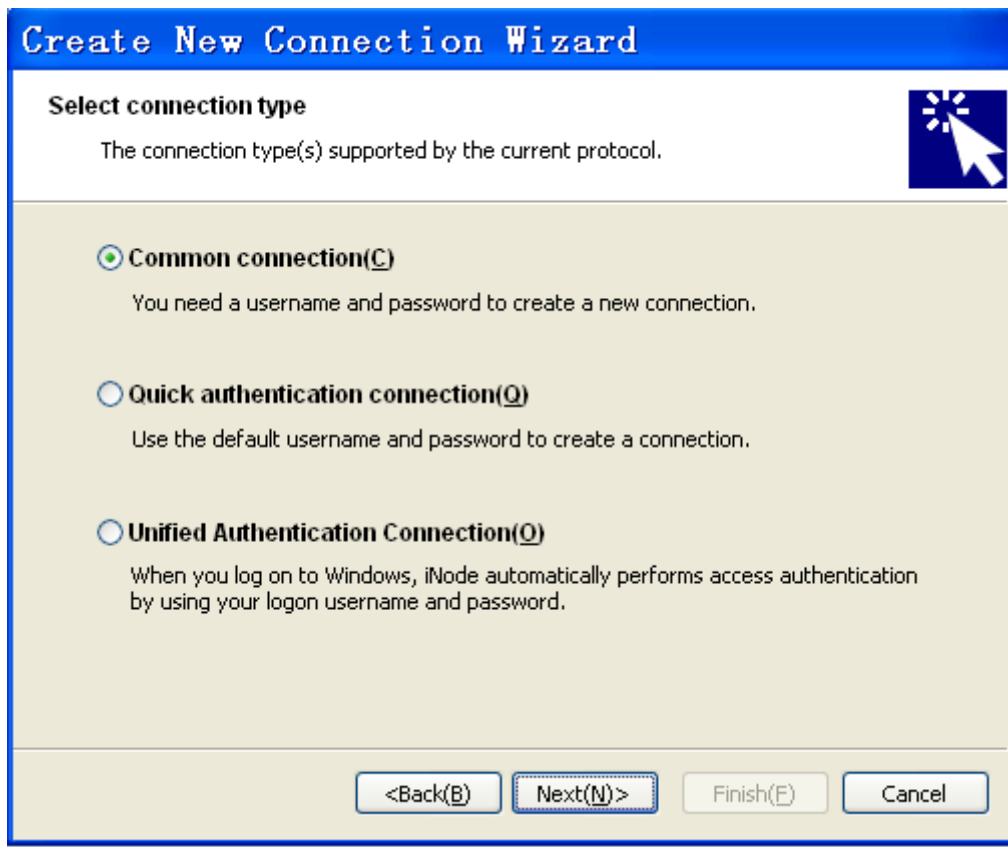
4. Click **New**.
5. On the **Create New Connection Wizard** window, select **802.1X protocol**, and then click **Next**.

Figure 231 Creating a new connection



6. Select the connection type **Common connection**, and click **Next**.

Figure 232 Selecting the connection type



7. Enter the username **usera** and the password **aaa**, and click **Next**.

Figure 233 Entering the username and the password

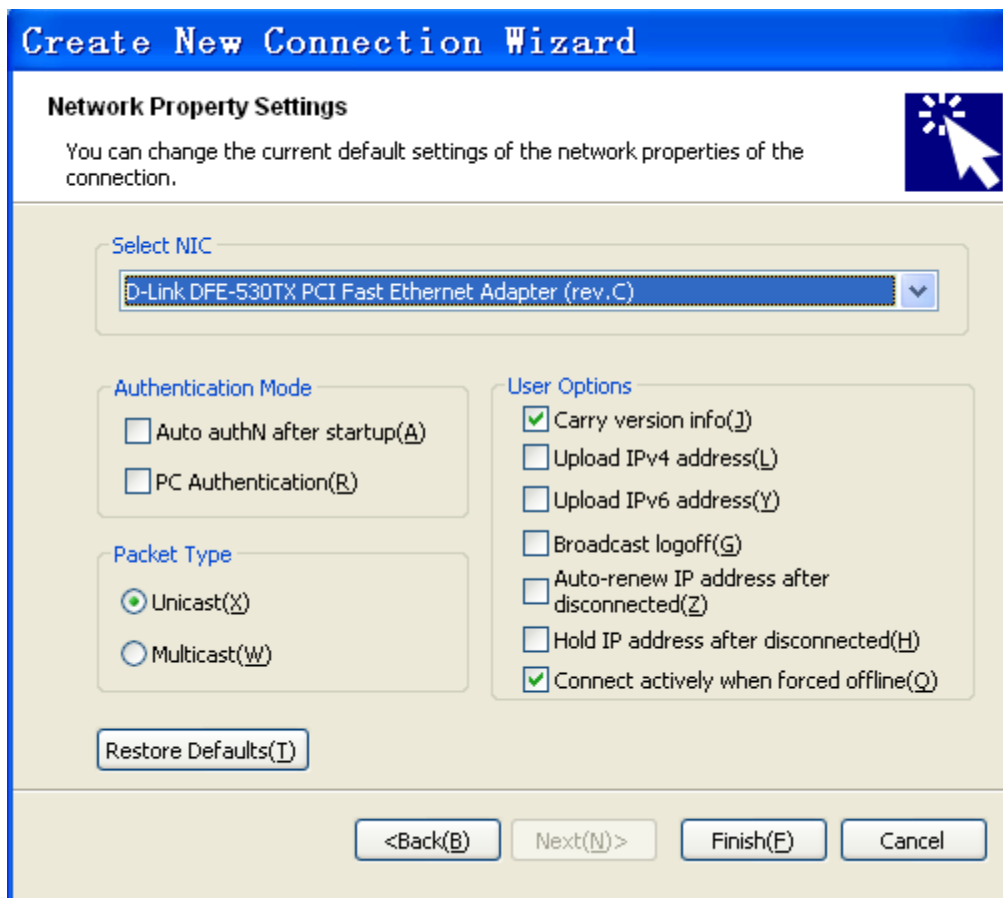
The screenshot shows a Windows-style dialog box titled "Create New Connection Wizard". The current step is "Account Information", which includes the instruction: "Input user name and password for network access, and certificate in order to enhance communication security." The form contains the following fields and options:

- Connection name(C): My 802.1X Connection
- Username(U): usera
- Password(P): \*\*\*
- Save username and password(V)
- Domain(D): [Empty dropdown menu]
- Enable advanced authentication(E)
  - MAC authentication(M)
  - Smart Card authentication(K)
  - Certificate authentication(I)
- Settings(S)... button

At the bottom of the dialog are four buttons: "<Back(B)", "Next(N)>", "Finish(F)", and "Cancel".

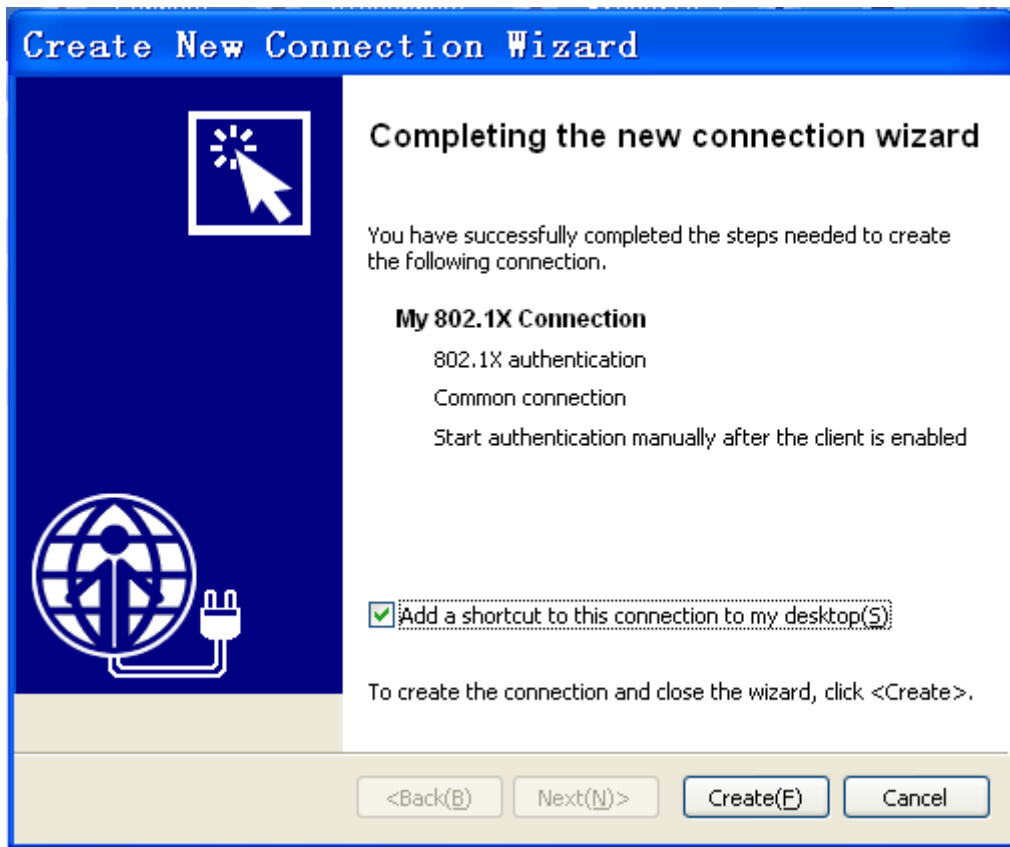
8. Select the NIC from the **Select NIC** list, use the default settings for other parameters, and click **Finish**.

Figure 234 Configuring network property settings



9. Click **Create** to create the connection.

Figure 235 Completing the new connection wizard



10. On the iNode client, click **My 802.1X Connection**, and then click **Connect** on the tool bar to initiate the connection.

### Configuring Host B


1. Configure the IP address of Host B as 192.168.3.2 with the subnet mask 255.255.255.0 and default gateway 192.168.3.1/24. (You can also use a DHCP server to assign an IP address on the subnet 192.168.3.1/24 to the host.)
2. Configure the iNode client on Host B in the same way the iNode client on Host A is configured. Configure the username as **userb** and the password as **bbb**.

### Configuring Host C

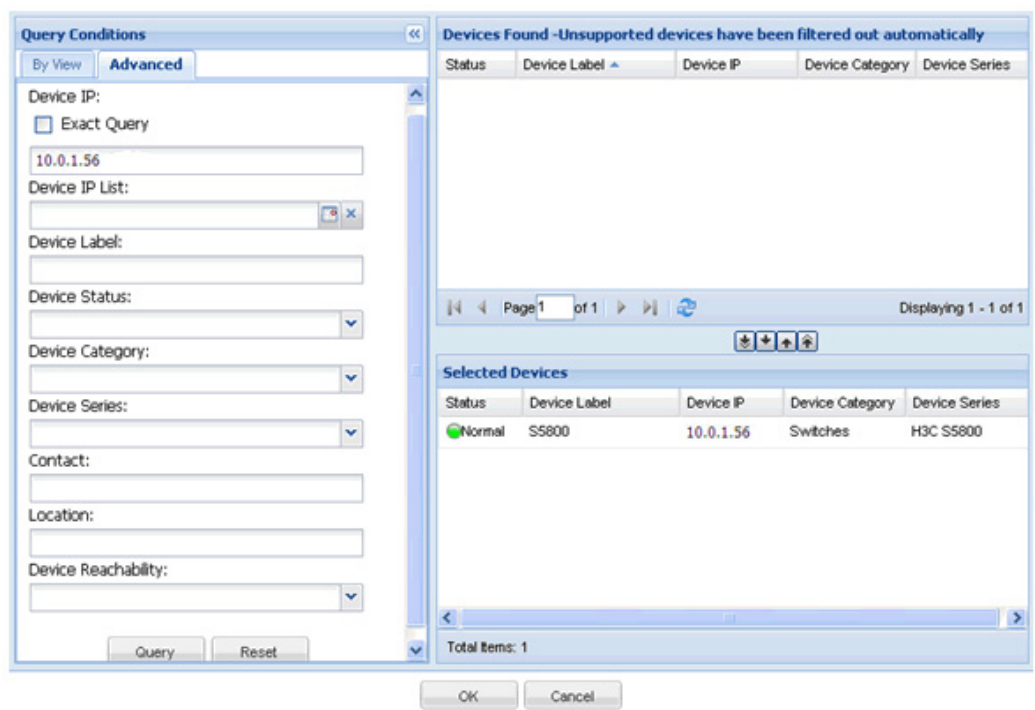
1. Configure the IP address of Host C as 192.168.4.2 with the subnet mask 255.255.255.0 and default gateway as 192.168.4.1/24. You can also use a DHCP server to assign an IP address on the subnet 192.168.4.1/24 to the host.
2. Configure the iNode client on Host C in the same way the iNode client on Host A is configured. Configure the username as **userc** and the password as **ccc**.

### Configuring the RADIUS server

1. Add Device A to IMC as an access device:
  - a. Click the **Service** tab.

- b. From the left navigation tree, select **User Access Manager > Access Device Management > Access Device**.
- c. Click **Add**.  
The page for adding access devices appears.
- d. Click **Select**.  
The page for selecting access devices appears.
- e. In the **Query Conditions** area, enter **10.0.1.56** (IP address of VLAN-interface 1 on Device A) in the **Device IP** field, and click **Query**.  
Device A appears in the **Devices Found** area.
- f. Select Device A in the **Devices Found** area and click the  icon.  
Device A is added to the **Selected Devices** area.
- g. Click **OK**.  
The page for adding access devices appears again.

**Figure 236** Selecting an access device



- h. Configure the shared key as **expert** and use default settings for other parameters.
  - i. Click **OK**.  
The access device has been added to IMC.
2. Add access rules:
    - a. Click the **Service** tab.

- b. From the left navigation tree, select **User Access Manager > Access Rule Management**.
- c. Click **Add**.
- d. In the **Basic Information** area, enter **Deploy VLAN 2** in the **Access Rule Name** field and use default settings for other parameters.
- e. In the **Authorization Information** area, enter **2** in the **Deploy VLAN** field and use default settings for other parameters.
- f. Click **OK**.

**Figure 237 Adding an access rule**

Service >> User Access Manager >> Access Rule Management >> Add Access Rule

Basic Information	
* Access Rule Name	Deploy VLAN 2
* Service Group	Ungrouped
Description	

Authorization Information		
Access Period	None	* Allocate IP
Downstream Rate		Upstream Rate
Priority		<input type="checkbox"/> RSA Authentication
Certificate Authentication	<input checked="" type="radio"/> None <input type="radio"/> EAP	
Certificate Type	EAP-TLS AuthN	
Deploy VLAN	2	
<input type="checkbox"/> Deploy User Profile		Deploy User Group
<input type="checkbox"/> Deploy ACL		

- f. Configure access rules **Deploy VLAN 3** and **Deploy VLAN 4** in the same way access rule **Deploy VLAN 2** is configured.
3. Add services:
    - a. Click the **Service** tab.
    - b. From the left navigation tree, select **User Access Manager > Service configuration**.
    - c. Click **Add**.
    - d. Enter **serverA** in the **Service Name** field, select **Deploy VLAN 2** from the **Default Access Rule** list, and use default settings for other parameters.
    - e. Click **OK**.

**Figure 238 Adding a service**

Service >> User Access Manager >> Service Configuration >> Add Service Configuration

Basic Information			
* Service Name	serverA	Service Suffix	
* Service Group	Ungrouped	* Default Access Rule	Deploy VLAN 2
* Default Security Policy	Disable Security Policy	* Default Internet Access Configuration	Do not use
* Default Proprietary Attribute Assignment Policy	Do not use		
Description			
<input checked="" type="checkbox"/> Available	<input type="checkbox"/> Portal Fast Authentication on Endpoints		



- f. Add the service **serverB** with the default access rule **Deploy VLAN 3** in the same way service **serverA** is configured.
  - g. Add the service **serverC** with the default access rule **Deploy VLAN 4** in the same way service **serverA** is configured.
4. Add access users:
- a. Click the **User** tab.
  - b. From the left navigation tree, select **Users > Add user**.  
The page for adding users appears.
  - c. Enter a username in the **User Name** field, enter an identity number in the **Identity Number** field, and use the default option for the **User Group** field.  
Make sure the combination of the username and the identity number is unique. The identity number can be the telephone number of the user so that the user can be contacted.
  - d. Click **OK**.

**Figure 239 Adding a user**

The screenshot shows a web interface for adding a user. The breadcrumb path is 'Users >> Add User'. The main heading is 'Add User'. Below it is a 'Basic Information' section with the following fields:

* User Name	<input type="text" value="H3C"/>	* Identity Number	<input type="text" value="123456"/>
Contact Address	<input type="text"/>	Telephone	<input type="text"/>
Email	<input type="text"/>	* User Group	<input type="text" value="Ungrouped"/>

At the bottom of the form are two buttons: 'OK' and 'Cancel'.

- a. From the left navigation tree, select **Access User View > All Access Users**.
- b. Click **Add**.  
The page for adding users appears.
- c. Click **Select**.
- d. On the user list that appears, query the user based on the username or the identity number.
- e. Select the user that meets the query criterion, and click **OK**.  
The username appears in the **User Name** field.
- f. Set the **Account Name** as **usera**, **Password** as **aaa**, select **serverA** as the associated access service for this user, and use the default settings for other parameters.
- g. Click **OK**.

Figure 240 Adding an access user

User >> All Access Users >> Add Access User

**Access account**

Access Information

\* User Name: H3C [Select] [Add User]

\* Account Name: usera

Trial Account  Computer User  Fast Access User

\* Password: ... Confirm Password: ...

Allow User to Change Password  Enable Password Strategy  Modify Password at Next Login

Expiration Date: [ ] Max. Smart Terminal Bindings for Portal: 1

Max. Idle Time: [ ] Minutes Max. Concurrent Logins: 1

Cell Phone Number: [ ] Cell Phone Password: [ ] Confirm Cell Phone Password: [ ]

Login Message: [ ]

Access Service

Service Name	Service Suffix	Default Security Policy	Status	Allocate IP
<input checked="" type="checkbox"/> serverA		Disable Security Policy	Available	

- k. Add users **userb** (with the password **bbb** and the associated access service **serverB**) and **userc** (with the password **ccc** and the associated access service **serverC**) in the same way the user **usera** is added.

## Verifying the configuration

# Verify that the users **usera**, **userb**, and **userc** can pass the 802.1X authentication and access the IP network.

# Verify that the MAC address-to-VLAN entries for Host A, Host B, and Host C have been correctly generated on Device A.

```
[DeviceA] display mac-vlan all
```

The following MAC VLAN addresses exist:

S:Static D:Dynamic

MAC ADDR	MASK	VLAN ID	PRIO	STATE
0011-0020-0001	ffff-ffff-ffff	2	0	D
0011-0020-0002	ffff-ffff-ffff	3	0	D
0011-0020-0003	ffff-ffff-ffff	4	0	D

-----

0011-0020-0001 ffff-ffff-ffff 2 0 D

0011-0020-0002 ffff-ffff-ffff 3 0 D

0011-0020-0003 ffff-ffff-ffff 4 0 D

Based on the MAC address-to-VLAN entries, the ports on Device A add VLAN tags to packets as follows:

- When the port GigabitEthernet 1/0/2 receives packets from Host A, the port tags the packets with VLAN 2.
- When the port GigabitEthernet 1/0/3 receives packets from Host B, the port tags the packets with VLAN 3.
- When the port GigabitEthernet 1/0/4 receives packets from Host C, the port tags the packets with VLAN 4.

# Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```
#
dot1x
#
interface Vlan-interface1
ip address 10.0.1.56 255.255.255.0
#
radius scheme macvlan
server-type extended
primary authentication 10.0.1.15
primary accounting 10.0.1.15
key authentication expert
key accounting expert
user-name-format without-domain
#
domain system
authentication lan-access radius-scheme macvlan
authorization lan-access radius-scheme macvlan
accounting lan-access radius-scheme macvlan
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type hybrid
port hybrid vlan 1 untagged
mac-vlan enable
dot1x
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type hybrid
port hybrid vlan 1 untagged
mac-vlan enable
dot1x
#
interface GigabitEthernet1/0/4
port link-mode bridge
port link-type hybrid
port hybrid vlan 1 untagged
mac-vlan enable
dot1x
#
interface GigabitEthernet1/0/5
port link-mode bridge
port link-type trunk
```

```
port trunk permit vlan 1 to 4
```

- Device B:

```
#
vlan 2 to 4
#
interface Vlan-interface2
 ip address 192.168.2.1 255.255.255.0
#
interface Vlan-interface3
 ip address 192.168.3.1 255.255.255.0
#
interface Vlan-interface4
 ip address 192.168.4.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 4
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 4
#
```

## Example: Configuring a super VLAN

### Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

# Network requirements

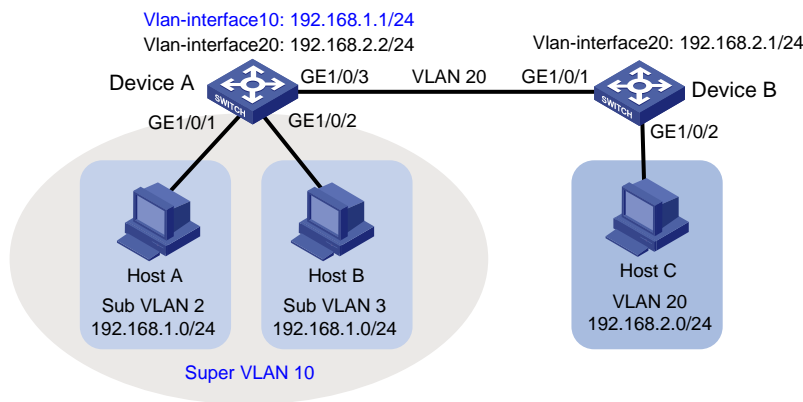
As shown in Figure 241:

- Users in VLAN 2 access the network through GigabitEthernet 1/0/1 of Device A. Users in VLAN 3 access the network through GigabitEthernet 1/0/2 of Device A.
- GigabitEthernet 1/0/3 of Device A and GigabitEthernet 1/0/1 of Device B belong to VLAN 20.
- The terminal users in VLAN 20 use IP addresses on the IP network segment 192.168.2.0/24, and they use 192.168.2.1 as the gateway IP address.

Configure a super VLAN to meet the following requirements:

- The terminal users in VLAN 2 and VLAN 3 use IP addresses on the IP network segment 192.168.1.0/24, and they use 192.168.1.1 as the gateway IP address.
- Terminal users in VLAN 2, VLAN 3, and VLAN 20 are isolated at Layer 2, and they can communicate with each other at Layer 3.

Figure 241 Network diagram



## Configuration restrictions and guidelines

You cannot assign physical ports to a super VLAN. A VLAN that contains physical ports cannot be configured as a super VLAN.

## Configuration procedures

### Configuring Device A

# Create VLAN 10, and configure the VLAN as a super VLAN.

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

# Create VLAN 2, and assign the port GigabitEthernet 1/0/1 to VLAN 2.

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

# Create VLAN 3, and assign the port GigabitEthernet 1/0/2 to VLAN 3.

```
[DeviceA] vlan 3
[DeviceA-vlan3] port gigabitethernet 1/0/2
[DeviceA-vlan3] quit
```

# Associate the super VLAN 10 with sub VLANs 2 and 3.

```
[DeviceA] vlan 10
[DeviceA-vlan10] subvlan 2 3
[DeviceA-vlan10] quit
```

# Create a VLAN interface for super VLAN 10.

```
[DeviceA] interface vlan-interface 10
```

# Configure an IP address for the VLAN interface.

```
[DeviceA-Vlan-interface10] ip address 192.168.1.1 24
```

# Enable local proxy ARP for the VLAN interface.

```
[DeviceA-Vlan-interface10] local-proxy-arp enable
[DeviceA-Vlan-interface10] quit
```

# Create VLAN 20.

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

# Configure GigabitEthernet 1/0/3 as a trunk port.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
```

# Remove GigabitEthernet 1/0/3 from VLAN 1.

```
[DeviceA-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

# Assign GigabitEthernet 1/0/3 to VLAN 20.

```
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 20
```

# Create a VLAN interface for VLAN 20.

```
[DeviceA] interface Vlan-interface 20
```

# Configure an IP address for the VLAN interface.

```
[DeviceA-Vlan-interface20] ip address 192.168.2.2 24
[DeviceA-Vlan-interface20] quit
```

## Configuring Device B

# Create VLAN 20.

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

# Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

```

Remove GigabitEthernet 1/0/1 from VLAN 1.
[DeviceB-GigabitEthernet1/0/1] undo port trunk permit vlan 1

Assign GigabitEthernet 1/0/1 to VLAN 20.
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 20

Assign GigabitEthernet 1/0/2 to VLAN 20.
[DeviceB] vlan 20
[DeviceB-vlan20] port gigabitethernet 1/0/2
[DeviceB-vlan20] quit

Create a VLAN interface for VLAN 20.
[DeviceB] interface Vlan-interface 20

Configure an IP address for the VLAN interface.
[DeviceB-Vlan-interface20] ip address 192.168.2.1 24
[DeviceB-Vlan-interface20] quit

```

## Verifying the configuration

```

Display the super VLAN configuration information.

```

```

[DeviceA] display supervlan
SuperVLAN ID : 10
SubVLAN ID : 2 3

```

```

VLAN ID: 10
VLAN Type: static
It is a Super VLAN.
Route Interface: configured
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Description: VLAN 0010
Name: VLAN 0010
Tagged Ports: none
Untagged Ports: none

```

```

VLAN ID: 2
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Description: VLAN 0002
Name: VLAN 0002
Tagged Ports: none
Untagged Ports:
 GigabitEthernet1/0/1

```

```

VLAN ID: 3

```

```
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged Ports: none
Untagged Ports:
GigabitEthernet1/0/2
```

# Verify that Host A and Host B can ping each other. In the ARP table of Host A, the IP address of Host B corresponds to the MAC address of VLAN-interface 10. In the ARP table of Host B, the IP address of Host A corresponds to the MAC address of VLAN-interface 10.

# Verify that Host A and Host C can ping each other. In the ARP table of Host A, no entry about Host C exists. In the ARP table of Host C, no entry about Host A exists.

## Configuration files

- Device A:

```
#
vlan 2
#
vlan 3
#
vlan 10
 supervlan
 subvlan 2 3
#
vlan 20
#
interface Vlan-interface10
 ip address 192.168.1.1 255.255.255.0
 local-proxy-arp enable
#
interface Vlan-interface20
 ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
```



```
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 20
```

- Device B:

```
#
vlan 20
#
interface Vlan-interface20
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
```

## Example: Configuring an isolate-user-VLAN

### Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

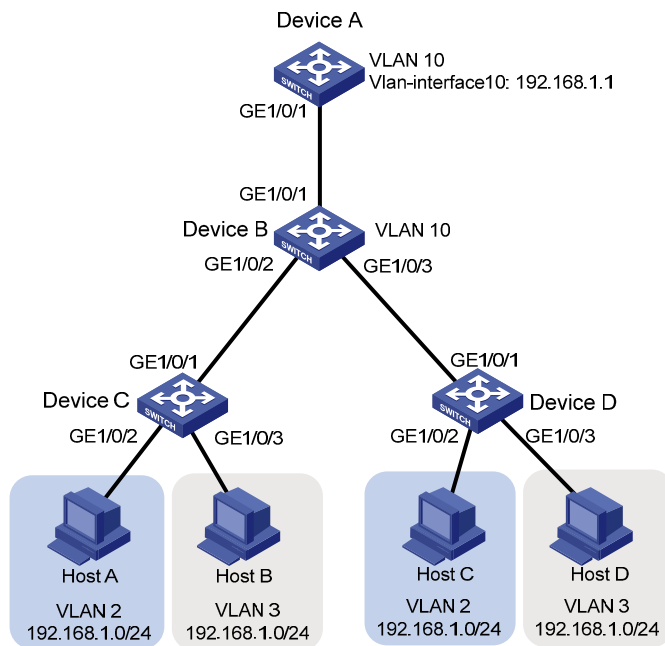
### Network requirements

As shown in [Figure 242](#), users in VLAN 2 and VLAN 3 are on the subnet 192.168.1.0/24.

Configure an isolate-user-VLAN to meet the following requirements:

- VLAN 2 and VLAN 3 are associated with the isolate-user-VLAN 10. The uplink device is aware of only VLAN 10.
- VLAN 2 and VLAN 3 are isolated at Layer 2 but interoperable at Layer 3.
- Users in the secondary VLAN 2 are interoperable at Layer 2.
- Secondary VLAN 3 users connected to Device C and Device D are isolated at Layer 2 but interoperable at Layer 3.

Figure 242 Network diagram



## Requirements analysis

To meet the network requirements, perform the following tasks:

- To implement Layer 3 communication between VLAN 2 and VLAN3, and between Layer 2 isolated users in the secondary VLAN 3, enable local proxy ARP on VLAN-interface 10 on Device A.
- To implement Layer 2 isolation between secondary VLAN 3 users that are connected to Device C and Device D, configure Layer 2 isolation between ports in this secondary VLAN.

## Configuration restrictions and guidelines

When you configure an isolate-user-VLAN, follow these restriction and guidelines:

- For the Layer 2 isolation between ports in a secondary VLAN to take effect, make sure the following conditions are true:
  - The ports in the secondary VLAN operate in host mode.
  - The isolate-user-VLAN is associated with the secondary VLAN.
- After you complete the isolate-user-VLAN configurations, make sure the isolate-user-VLAN is the PVID of the uplink port and the secondary VLAN is the PVID of the downlink port. HP recommends that you assign the following hybrid ports to the VLANs in untagged mode:
  - Hybrid ports that have been assigned to the isolate-user-VLAN in tagged mode.
  - Hybrid ports that have been assigned to the secondary VLANs in tagged mode.

# Configuration procedures

## Configuring Device A

# Create VLAN 10.

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

# Create VLAN-interface 10, and assign the IP address 192.168.1.1/24 to this interface.

```
[DeviceA] interface Vlan-interface 10
[DeviceA-Vlan-interface10] ip address 192.168.1.1 24
```

# Enable the local proxy ARP on VLAN-interface 10.

```
[DeviceA-Vlan-interface10] local-proxy-arp enable
[DeviceA-Vlan-interface10] quit
```

# Configure the port GigabitEthernet 1/0/1 as a hybrid port.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

# Configure the port GigabitEthernet 1/0/1 as an untagged member of VLAN 10.

```
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 10 untagged
```

# Configure the PVID of the port GigabitEthernet 1/0/1 as 10.

```
[DeviceA-GigabitEthernet1/0/1] port hybrid pvid vlan 10
[DeviceA-GigabitEthernet1/0/1] quit
```

## Configuring Device B

# Create VLAN 10 and configure VLAN 10 as an isolate-user-VLAN.

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] isolate-user-vlan enable
[DeviceB-vlan10] quit
```

# Configure the port GigabitEthernet 1/0/1 to operate in promiscuous mode in VLAN 10.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port isolate-user-vlan 10 promiscuous
[DeviceB-GigabitEthernet1/0/1] quit
```

# Create VLAN 2 and VLAN 3.

```
[DeviceB] vlan 2 to 3
```

# Configure Layer 2 isolation between ports in VLAN 3.

```
[DeviceB] vlan 3
[DeviceB-vlan3] isolated-vlan enable
```

# Configure the port GigabitEthernet 1/0/2 as a trunk port.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
```

# Assign the port GigabitEthernet 1/0/2 to VLANs 2 and 3.

```

[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2 3
Configure the port GigabitEthernet 1/0/2 to operate in host mode.
[DeviceB-GigabitEthernet1/0/2] port isolate-user-vlan host
[DeviceB-GigabitEthernet1/0/2] quit

Configure the port GigabitEthernet 1/0/3 as a trunk port.
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk

Assign the port GigabitEthernet 1/0/3 to VLANs 2 and 3.
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 2 3

Configure the port GigabitEthernet 1/0/3 to operate in host mode.
[DeviceB-GigabitEthernet1/0/3] port isolate-user-vlan host
[DeviceB-GigabitEthernet1/0/3] quit

Associate the isolate-user-VLAN 10 with secondary VLANs 2 and 3.
[DeviceB] isolate-user-vlan 10 secondary 2 3

```

## Configuring Device C

```

Create VLAN 10 and configure this VLAN as an isolate-user-VLAN.
<DeviceC> system-view
[DeviceC] vlan 10
[DeviceC-vlan10] isolate-user-vlan enable
[DeviceC-vlan10] quit

Create VLAN 2 and VLAN 3.
[DeviceC] vlan 2 to 3

Configure Layer 2 isolation between ports in VLAN 3.
[DeviceC] vlan 3
[DeviceC-vlan3] isolated-vlan enable

Configure the port GigabitEthernet 1/0/1 as a trunk port.
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk

Assign the port GigabitEthernet 1/0/1 to VLANs 2, 3, and 10.
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 2 3 10
[DeviceC-GigabitEthernet1/0/1] quit

Assign the port GigabitEthernet 1/0/2 to VLAN 2.
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port access vlan 2

Configure the port GigabitEthernet 1/0/2 to operate in host mode.
[DeviceC-GigabitEthernet1/0/2] port isolate-user-vlan host
[DeviceC-GigabitEthernet1/0/2] quit

Assign the port GigabitEthernet 1/0/3 to VLAN 3.
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port access vlan 3

```

```
Configure the port GigabitEthernet 1/0/3 to operate in host mode.
[DeviceC-GigabitEthernet1/0/3] port isolate-user-vlan host
[DeviceC-GigabitEthernet1/0/3] quit

Associate the isolate-user-VLAN 10 with secondary VLANs 2 and 3.
[DeviceC] isolate-user-vlan 10 secondary 2 3
```

## Configuring Device D

Configure Device D in the same way Device C is configured. (Details not shown.)

## Verifying the configuration

```
Display the isolate-user-VLAN configuration on Device B.
```

```
[DeviceB] display isolate-user-vlan
Isolate-user-VLAN VLAN ID : 10
Secondary VLAN ID : 2-3

VLAN ID: 10
VLAN Type: static
Isolate-user-VLAN type: isolate-user-VLAN
Route Interface: not configured
Description: VLAN 0010
Name: VLAN 0010
Tagged Ports:
 GigabitEthernet1/0/2 GigabitEthernet1/0/3
Untagged Ports:
 GigabitEthernet1/0/1

VLAN ID: 2
VLAN Type: static
Isolate-user-VLAN type: secondary
Route Interface: not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged Ports:
 GigabitEthernet1/0/2 GigabitEthernet1/0/3
Untagged Ports:
 GigabitEthernet1/0/1

VLAN ID: 3
VLAN Type: static
Isolate-user-VLAN type: isolated secondary
Route Interface: not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged Ports:
 GigabitEthernet1/0/2 GigabitEthernet1/0/3
```

```
Untagged Ports:
 GigabitEthernet1/0/1
```

# Display the isolate-user-VLAN configuration on Device C.

```
[DeviceC] display isolate-user-vlan
Isolate-user-VLAN VLAN ID : 10
Secondary VLAN ID : 2-3
```

```
VLAN ID: 10
VLAN Type: static
Isolate-user-VLAN type: isolate-user-VLAN
Route Interface: not configured
Description: VLAN 0010
Name: VLAN 0010
Tagged Ports:
 GigabitEthernet1/0/1
Untagged Ports:
 GigabitEthernet1/0/2 GigabitEthernet1/0/3
```

```
VLAN ID: 2
VLAN Type: static
Isolate-user-VLAN type: secondary
Route Interface: not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged Ports:
 GigabitEthernet1/0/1
Untagged Ports:
 GigabitEthernet1/0/2
```

```
VLAN ID: 3
VLAN Type: static
Isolate-user-VLAN type: isolated secondary
Route Interface: not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged Ports:
 GigabitEthernet1/0/1
Untagged Ports:
GigabitEthernet1/0/3
```

# Verify that Host A can successfully ping Host B. In the ARP table of Host A, the IP address of Host B corresponds to the MAC address of VLAN-interface 10 on Device A.

# Verify that Host A can successfully ping Host C. An entry for the IP address of Host C exists in the ARP table of Host A. The associated MAC address might be the MAC address of VLAN-interface 10 on Device A, or the MAC address of Host C.

# Verify that Host B can successfully ping Host D. In the ARP table of Host B, the IP address of Host D corresponds to the MAC address of VLAN-interface 10 on Device A.

# Configuration files

The HP 5500 SI Switch Series does not support the **port link-mode bridge** command.

- Device A:

```
#
vlan 10
#
interface Vlan-interface10
 ip address 192.168.1.1 255.255.255.0
 local-proxy-arp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 10 untagged
 port hybrid pvid vlan 10
#
```

- Device B:

```
#
vlan 2
#
vlan 3
 isolated-vlan enable
#
vlan 10
 isolate-user-vlan enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port isolate-user-vlan 10 promiscuous
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2 to 3 10 untagged
 port hybrid pvid vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port isolate-user-vlan host
 port link-type trunk
 port trunk permit vlan 1 to 3 10
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port isolate-user-vlan host
 port link-type trunk
 port trunk permit vlan 1 to 3 10
```

```
#
isolate-user-vlan 10 secondary 2 to 3
#
```

- **Device C:**

```
#
vlan 2
#
vlan 3
 isolated-vlan enable
#
vlan 10
 isolate-user-vlan enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 3 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port isolate-user-vlan host
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2 10 untagged
 port hybrid pvid vlan 2
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port isolate-user-vlan host
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 3 10 untagged
 port hybrid pvid vlan 3
#
isolate-user-vlan 10 secondary 2 to 3
#
```

- **Device D:**

The configuration files on Device D are the same as the configuration files on Device C. (Details not shown.)



# VLAN mapping configuration examples

This chapter provides VLAN mapping configuration examples.

VLAN mapping re-marks VLAN tagged traffic with new VLAN IDs. HP provides the following types of VLAN mapping:

- **One-to-one VLAN mapping**—Replaces one VLAN tag with another.
- **Two-to-two VLAN mapping**—Replaces the outer and inner VLAN tags of double tagged traffic with a new pair of VLAN tags.

## Example: Configuring one-to-one VLAN mapping

### Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

### Network requirements

As shown in [Figure 243](#):

- Two branches of a company, Site 1 and Site 2, communicate with each other through the service provider network. The company uses CVLAN 10 to transmit voice traffic and uses CVLAN 20 to transmit data traffic.
- PE 1 and PE 2 are the edge devices of the service provider network. The service provider allocates only SVLAN 100 and SVLAN 200 to the company for transmitting data.

Configure one-to-one VLAN mapping, so that Site 1 and Site 2 can use SVLAN 100 and SVLAN 200 to transmit the voice traffic and data traffic, respectively, between the two branches. [Figure 244](#) shows the effect of the one-to-one VLAN mapping.

Figure 243 Network diagram

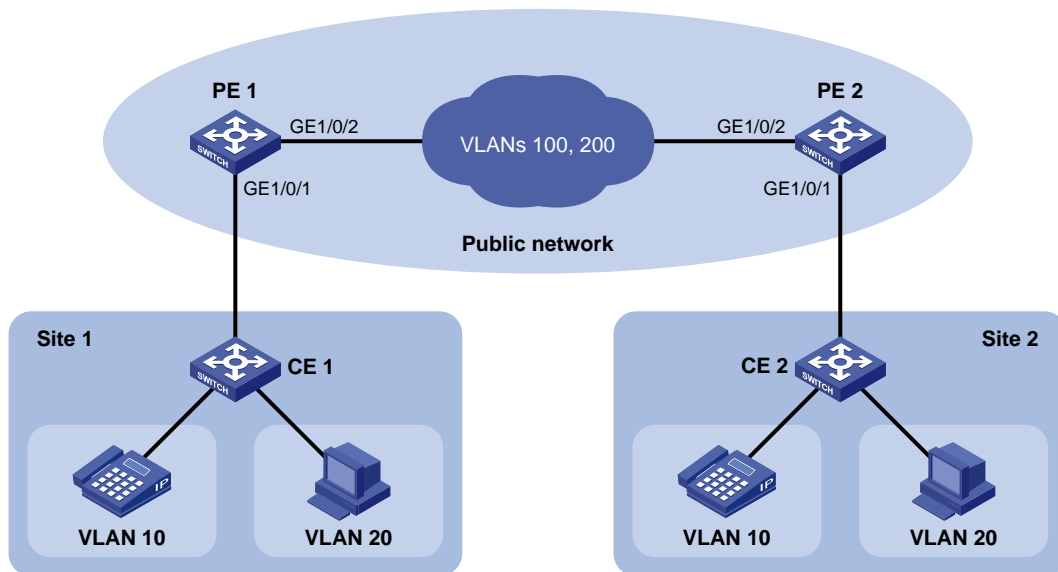
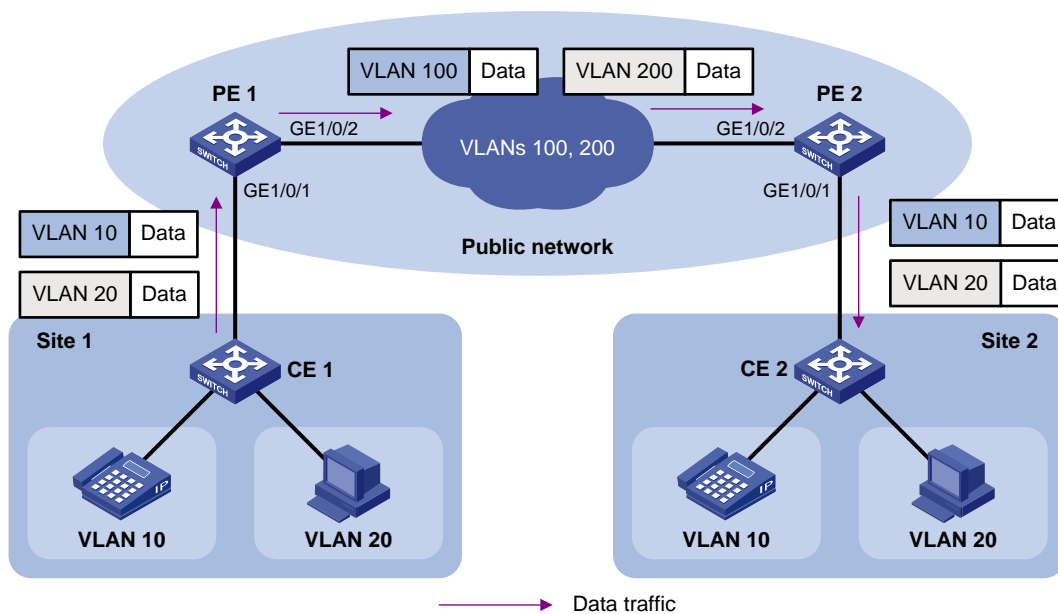


Figure 244 One-to-one VLAN mapping effect



## Configuration restrictions and guidelines

When you configure one-to-one VLAN mapping, you must enable basic QinQ on the customer-side ports.

# Configuration procedures

## Configuring PE 1

1. Create the CVLANs and SVLANs used in this example.

```
<PE1> system-view
[PE1] vlan 10
[PE1-vlan10] quit
[PE1] vlan 20
[PE1-vlan20] quit
[PE1] vlan 100
[PE1-vlan100] quit
[PE1] vlan 200
[PE1-vlan200] quit
```

2. Configure an uplink policy:

# Configure a class named **uplink10** to match the traffic from CVLAN 10 of Site 1.

```
[PE1] traffic classifier uplink10
[PE1-classifier-uplink10] if-match customer-vlan-id 10
[PE1-classifier-uplink10] quit
```

# Configure a behavior named **remark\_to\_100** to mark traffic with SVLAN tag 100.

```
[PE1] traffic behavior remark_to_100
[PE1-behavior-remark_to_100] remark service-vlan-id 100
[PE1-behavior-remark_to_100] quit
```

# Configure a class named **uplink20** to match the traffic from CVLAN 20.

```
[PE1] traffic classifier uplink20
[PE1-classifier-uplink20] if-match customer-vlan-id 20
[PE1-classifier-uplink20] quit
```

# Configure a behavior named **remark\_to\_200** to mark traffic with SVLAN tag 200.

```
[PE1] traffic behavior remark_to_200
[PE1-behavior-remark_to_200] remark service-vlan-id 200
[PE1-behavior-remark_to_200] quit
```

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

```
[PE1] qos policy uplink
```

# Associate class **uplink10** with behavior **remark\_to\_100**.

```
[PE1-qospolicy-uplink] classifier uplink10 behavior remark_to_100
```

# Associate class **uplink20** with behavior **remark\_to\_200**.

```
[PE1-qospolicy-uplink] classifier uplink20 behavior remark_to_200
[PE1-qospolicy-uplink] quit
```

3. Configure a downlink policy:

# Configure a class named **downlink100** to match the traffic from SVLAN 100.

```
[PE1] traffic classifier downlink100
[PE1-classifier-downlink100] if-match service-vlan-id 100
[PE1-classifier-downlink100] quit
```

# Configure a behavior named **remark\_to\_10** to mark traffic with CVLAN tag 10.

```
[PE1] traffic behavior remark_to_10
[PE1-behavior-remark_to_10] remark customer-vlan-id 10
[PE1-behavior-remark_to_10] quit
```

# Configure a class named **downlink200** to match the traffic from CVLAN 200.

```
[PE1] traffic classifier downlink200
[PE1-classifier-downlink200] if-match service-vlan-id 200
[PE1-classifier-downlink200] quit
```

# Configure a behavior named **remark\_to\_20** to mark traffic with CVLAN tag 20.

```
[PE1] traffic behavior remark_to_20
[PE1-behavior-remark_to_20] remark customer-vlan-id 20
[PE1-behavior-remark_to_20] quit
```

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

```
[PE1] qos policy downlink
```

# Associate class **downlink100** with behavior **remark\_to\_10**.

```
[PE1-qospolicy-downlink] classifier downlink100 behavior remark_to_10
```

# Associate class **downlink200** with behavior **remark\_to\_20**.

```
[PE1-qospolicy-downlink] classifier downlink200 behavior remark_to_20
[PE1-qospolicy-downlink] quit
```

#### 4. Configure the customer-side port GigabitEthernet 1/0/1:

# Configure GigabitEthernet 1/0/1 as a hybrid port.

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type hybrid
```

# Configure GigabitEthernet 1/0/1 to permit the packets from VLANs 10, 20, 100, and 200 to pass through tagged.

```
[PE1-GigabitEthernet1/0/1] port hybrid vlan 10 20 100 200 tagged
```

# Remove GigabitEthernet 1/0/1 from VLAN 1.

```
[PE1-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

# Enable basic QinQ on GigabitEthernet 1/0/1.

```
[PE1-GigabitEthernet1/0/1] qinq enable
```

# Apply the policy named **uplink** to the incoming traffic of GigabitEthernet 1/0/1.

```
[PE1-GigabitEthernet1/0/1] qos apply policy uplink inbound
```

# Apply the policy named **downlink** to the outgoing traffic of GigabitEthernet 1/0/1.

```
[PE1-GigabitEthernet1/0/1] qos apply policy downlink outbound
[PE1-GigabitEthernet1/0/1] quit
```

#### 5. Configure the network-side port GigabitEthernet 1/0/2:

# Configure the network-side port GigabitEthernet 1/0/2 as a trunk port.

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
```

# Assign GigabitEthernet 1/0/2 to VLANs 100 and 200.

```
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

# Remove GigabitEthernet 1/0/2 from VLAN 1.

```
[PE1-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[PE1-GigabitEthernet1/0/2] quit
```

## Configuring PE 2

1. Create the CVLANs and SVLANs used in this example.

```
<PE2> system-view
[PE2] vlan 10
[PE2-vlan10] quit
[PE2] vlan 20
[PE2-vlan20] quit
[PE2] vlan 100
[PE2-vlan100] quit
[PE2] vlan 200
[PE2-vlan200] quit
```

2. Configure an uplink policy:

# Configure a class named **uplink10** to match the traffic from CVLAN 10 of Site 2.

```
[PE2] traffic classifier uplink10
[PE2-classifier-uplink10] if-match customer-vlan-id 10
[PE2-classifier-uplink10] quit
```

# Configure a behavior named **remark\_to\_100** to mark traffic with SVLAN tag 100.

```
[PE2] traffic behavior remark_to_100
[PE2-behavior-remark_to_100] remark service-vlan-id 100
[PE2-behavior-remark_to_100] quit
```

# Configure a class named **uplink20** to match the traffic from CVLAN 20.

```
[PE2] traffic classifier uplink20
[PE2-classifier-uplink20] if-match customer-vlan-id 20
[PE2-classifier-uplink20] quit
```

# Configure a behavior named **remark\_to\_200** to mark traffic with SVLAN tag 200.

```
[PE2] traffic behavior remark_to_200
[PE2-behavior-remark_to_200] remark service-vlan-id 200
[PE2-behavior-remark_to_200] quit
```

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

```
[PE2] qos policy uplink
```

# Associate class **uplink10** with behavior **remark\_to\_100**.

```
[PE2-qospolicy-uplink] classifier uplink10 behavior remark_to_100
```

# Associate class **uplink20** with behavior **remark\_to\_200**.

```
[PE2-qospolicy-uplink] classifier uplink20 behavior remark_to_200
[PE2-qospolicy-uplink] quit
```

3. Configure a downlink policy:

# Configure a class named **downlink100** to match the traffic from SVLAN 100.

```
[PE2] traffic classifier downlink100
[PE2-classifier-downlink100] if-match service-vlan-id 100
[PE2-classifier-downlink100] quit
```

# Configure a behavior named **remark\_to\_10** to mark traffic with CVLAN tag 10.

```

[PE2] traffic behavior remark_to_10
[PE2-behavior-remark_to_10] remark customer-vlan-id 10
[PE2-behavior-remark_to_10] quit
Configure a class named downlink200 to match the traffic from CVLAN 200.
[PE2] traffic classifier downlink200
[PE2-classifier-downlink200] if-match service-vlan-id 200
[PE2-classifier-downlink200] quit
Configure a behavior named remark_to_20 to mark traffic with CVLAN tag 20.
[PE2] traffic behavior remark_to_20
[PE2-behavior-remark_to_20] remark customer-vlan-id 20
[PE2-behavior-remark_to_20] quit
Create a QoS policy named downlink.
[PE2] qos policy downlink
Associate class downlink100 with behavior remark_to_10.
[PE2-qospolicy-downlink] classifier downlink100 behavior remark_to_10
Associate class downlink200 with behavior remark_to_20.
[PE2-qospolicy-downlink] classifier downlink200 behavior remark_to_20
[PE2-qospolicy-downlink] quit

```

4. Configure the customer-side port GigabitEthernet 1/0/1:

```

Configure GigabitEthernet 1/0/1 as a hybrid port.
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] port link-type hybrid
Configure GigabitEthernet 1/0/1 to permit the packets from VLANs 10, 20, 100, and 200 to
pass through tagged.
[PE2-GigabitEthernet1/0/1] port hybrid vlan 10 20 100 200 tagged
Remove GigabitEthernet 1/0/1 from VLAN 1.
[PE2-GigabitEthernet1/0/1] undo port hybrid vlan 1
Enable basic QinQ on GigabitEthernet 1/0/1.
[PE2-GigabitEthernet1/0/1] qinq enable
Apply the policy named uplink to the incoming traffic of GigabitEthernet 1/0/1.
[PE2-GigabitEthernet1/0/1] qos apply policy uplink inbound
Apply the policy named downlink to the outgoing traffic of GigabitEthernet 1/0/1.
[PE2-GigabitEthernet1/0/1] qos apply policy downlink outbound
[PE2-GigabitEthernet1/0/1] quit

```

5. Configure the network-side port GigabitEthernet 1/0/2:

```

Configure the network-side port GigabitEthernet 1/0/2 as a trunk port.
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
Assign GigabitEthernet 1/0/2 to VLANs 100 and 200.
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100 200
Remove GigabitEthernet 1/0/2 from VLAN 1.
[PE2-GigabitEthernet1/0/2] undo port trunk permit vlan 1

```

```
[PE2-GigabitEthernet1/0/2] quit
```

## Configuring other devices in the service provider network

Configure all ports on the path between PE 1 and PE 2 to allow frames from VLANs 100 and 200 to pass through without removing the SVLAN tags.

## Verifying the configuration

# Display the port configurations. This example uses GigabitEthernet 1/0/1 on PE 1.

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1]display this
port link-mode bridge
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 10 20 100 200 tagged
qinq enable
qos apply policy uplink inbound
qos apply policy downlink outbound
#
return
```

# Verify that the policies have been successfully applied to ports. This example uses GigabitEthernet 1/0/1 on PE 1.

```
[PE1]display qos policy interface GigabitEthernet 1/0/1
```

```
Interface: GigabitEthernet1/0/1
```

```
Direction: Inbound
```

```
Policy: uplink
```

```
Classifier: uplink10
```

```
Operator: AND
```

```
Rule(s) : If-match customer-vlan-id 10
```

```
Behavior: remark_to_100
```

```
Marking:
```

```
Remark Service VLAN ID 100
```

```
Classifier: uplink20
```

```
Operator: AND
```

```
Rule(s) : If-match customer-vlan-id 20
```

```
Behavior: remark_to_200
```

```
Marking:
```

```
Remark Service VLAN ID 200
```

```
Direction: Outbound
```

```
Policy: downlink
```

```
Classifier: downlink100
```

```
Operator: AND
```

```

Rule(s) : If-match service-vlan-id 100
Behavior: remark_to_10
Marking:
 Remark Customer VLAN ID 10
Classifier: downlink200
Operator: AND
Rule(s) : If-match service-vlan-id 200
Behavior: remark_to_20
Marking:
 Remark Customer VLAN ID 20

```

## Configuration files

- PE 1:

```

#
vlan 10
#
vlan 20
#
vlan 100
#
vlan 200
#
traffic classifier uplink10 operator and
 if-match customer-vlan-id 10
traffic classifier uplink20 operator and
 if-match customer-vlan-id 20
traffic classifier downlink100 operator and
 if-match service-vlan-id 100
traffic classifier downlink200 operator and
 if-match service-vlan-id 200
#
traffic behavior remark_to_100
 remark service-vlan-id 100
traffic behavior remark_to_200
 remark service-vlan-id 200
traffic behavior remark_to_10
 remark customer-vlan-id 10
traffic behavior remark_to_20
 remark customer-vlan-id 20
#
qos policy uplink
 classifier uplink10 behavior remark_to_100
 classifier uplink20 behavior remark_to_200
qos policy downlink
 classifier downlink100 behavior remark_to_10
 classifier downlink200 behavior remark_to_20

```



```

#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 20 100 200 tagged
 qinq enable
 qos apply policy uplink inbound
 qos apply policy downlink outbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#

```

- PE 2:

```

#
vlan 10
#
vlan 20
#
vlan 100
#
vlan 200
#
traffic classifier uplink10 operator and
 if-match customer-vlan-id 10
traffic classifier uplink20 operator and
 if-match customer-vlan-id 20
traffic classifier downlink100 operator and
 if-match service-vlan-id 100
traffic classifier downlink200 operator and
 if-match service-vlan-id 200
#
traffic behavior remark_to_100
 remark service-vlan-id 100
traffic behavior remark_to_200
 remark service-vlan-id 200
traffic behavior remark_to_10
 remark customer-vlan-id 10
traffic behavior remark_to_20
 remark customer-vlan-id 20
#
qos policy uplink
 classifier uplink10 behavior remark_to_100
 classifier uplink20 behavior remark_to_200
qos policy downlink

```

```

classifier downlink100 behavior remark_to_10
classifier downlink200 behavior remark_to_20
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 10 20 100 200 tagged
qinq enable
qos apply policy uplink inbound
qos apply policy downlink outbound
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200
#

```

## Example: Configuring two-to-two VLAN mapping

### Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220

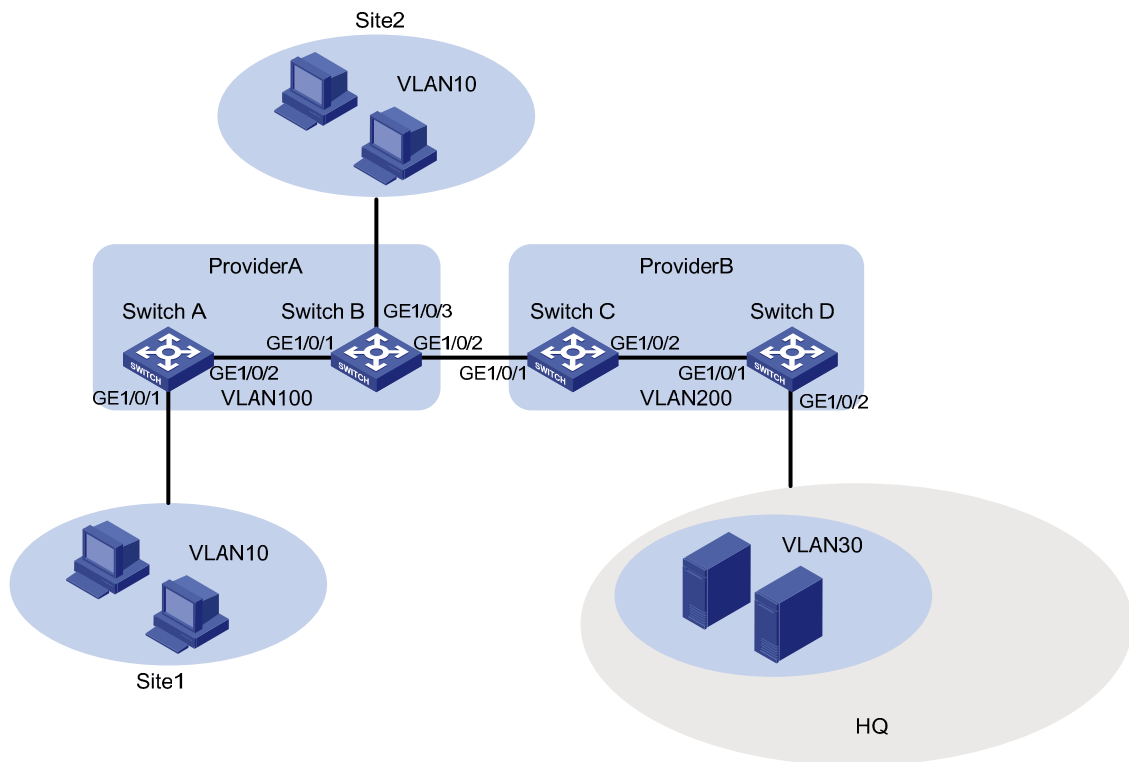
### Network requirements

As shown in [Figure 245](#):

- Site 1 and Site 2 are two branches of a company, and they both belong to VLAN 10. A VPN connection is set up between the two branches through the QinQ service of service provider A, which allocates SVLAN 100 to the company.
- After the company is acquired by another company, the two sites must access the network of the new company.
- The VPN service of the new company is provided by service provider B, which allocates SVLAN 200 to the new company.
- The headquarters of the new company uses VLAN 30 to provide services for the two sites.

Configure two-to-two VLAN mapping, so that the two sites can access VLAN 30 in the headquarters without changing the VLAN configurations for the sites and SVLANs.

Figure 245 Network diagram



## Configuration restrictions and guidelines

You need to configure two-to-two VLAN mapping on only one of the edge devices connecting the two service provider networks. This example uses Switch C.

## Configuration procedures

### Configuring Switch A

# Create VLAN 100.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] quit
```

# Configure QinQ on GigabitEthernet 1/0/1 to add outer VLAN tag 100 to packets from VLAN 10.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port access vlan 100
[SwitchA-GigabitEthernet1/0/1] qinq enable
[SwitchA-GigabitEthernet1/0/1] quit
```

# Configure the network-side port GigabitEthernet 1/0/2 as a trunk port.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
```

```
Assign GigabitEthernet 1/0/2 to VLAN 100.
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 100

Remove GigabitEthernet 1/0/2 from VLAN 1.
[SwitchA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[SwitchA-GigabitEthernet1/0/2] quit
```

## Configuring Switch B

```
Create VLAN 100.
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] quit

Configure QinQ on GigabitEthernet 1/0/3 to add outer VLAN tag 100 to packets from VLAN 10.
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port access vlan 100
[SwitchB-GigabitEthernet1/0/3] qinq enable
[SwitchB-GigabitEthernet1/0/3] quit

Configure GigabitEthernet 1/0/1 as a trunk port.
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk

Assign GigabitEthernet 1/0/1 to VLAN 100.
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 100

Remove GigabitEthernet 1/0/1 from VLAN 1.
[SwitchB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchB-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2 as a trunk port.
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type trunk

Assign GigabitEthernet 1/0/2 to VLAN 100.
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 100

Remove GigabitEthernet 1/0/2 from VLAN 1.
[SwitchB-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[SwitchB-GigabitEthernet1/0/2] quit
```

## Configuring Switch C

1. Create SVLAN 200.

```
<SwitchC> system-view
[SwitchC] vlan 200
[SwitchC-vlan200] quit
```
2. Configure VLAN mapping for the traffic received on GigabitEthernet 1/0/1:

```
Configure a class named uplink_in to match traffic with inner VLAN tag 10 and outer VLAN tag 100.
[SwitchC] traffic classifier uplink_in
[SwitchC-classifier-uplink_in] if-match customer-vlan-id 10
```

```
[SwitchC-classifier-uplink_in] if-match service-vlan-id 100
[SwitchC-classifier-uplink_in] quit
Configure a behavior named uplink_in to change the outer VLAN tag into VLAN tag 200.
[SwitchC] traffic behavior uplink_in
[SwitchC-behavior-uplink_in] remark service-vlan-id 200
[SwitchC-behavior-uplink_in] quit
Create a QoS policy named uplink_in.
[SwitchC] qos policy uplink_in
Associate class uplink_in with traffic behavior uplink_in in the QoS policy.
[SwitchC-qospolicy-uplink_in] classifier uplink_in behavior uplink_in
[SwitchC-qospolicy-uplink_in] quit
Configure GigabitEthernet 1/0/1 as a trunk port.
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
Assign GigabitEthernet 1/0/1 to VLAN 200.
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 200
Remove GigabitEthernet 1/0/1 from VLAN 1.
[SwitchC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
Apply QoS policy uplink_in to the incoming traffic of GigabitEthernet 1/0/1.
[SwitchC-GigabitEthernet1/0/1] qos apply policy uplink_in inbound
[SwitchC-GigabitEthernet1/0/1] quit
```

3. Configure VLAN mapping for the traffic sent out of GigabitEthernet 1/0/2:

# Configure a class named **uplink\_out** to match traffic with inner VLAN tag 10 and outer VLAN tag 200.

```
[SwitchC] traffic classifier uplink_out
[SwitchC-classifier-uplink_out] if-match customer-vlan-id 10
[SwitchC-classifier-uplink_out] if-match service-vlan-id 200
[SwitchC-classifier-uplink_out] quit
```

# Configure a behavior named **uplink\_out** to change the inner VLAN tag into VLAN tag 30.

```
[SwitchC] traffic behavior uplink_out
[SwitchC-behavior-uplink_out] remark customer-vlan-id 30
[SwitchC-behavior-uplink_out] quit
```

# Create a QoS policy named **uplink\_out**.

```
[SwitchC] qos policy uplink_out
```

# Associate class **uplink\_out** with traffic behavior **uplink\_out** in the QoS policy.

```
[SwitchC-qospolicy-uplink_out] classifier uplink_out behavior uplink_out
[SwitchC-qospolicy-uplink_out] quit
```

# Configure GigabitEthernet 1/0/2 as a trunk port.

```
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-type trunk
```

# Assign GigabitEthernet 1/0/2 to VLAN 200.

```
[SwitchC-GigabitEthernet1/0/2] port trunk permit vlan 200
```

# Remove GigabitEthernet 1/0/2 from VLAN 1.

```
[SwitchC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
```

# Apply QoS policy **uplink\_out** to the outgoing traffic of GigabitEthernet 1/0/2.

```
[SwitchC-GigabitEthernet1/0/2] qos apply policy uplink_out outbound
```

```
[SwitchC-GigabitEthernet1/0/2] quit
```

#### 4. Configure VLAN mapping for the traffic sent out of GigabitEthernet 1/0/1:

# Configure a class named **downlink\_out** to match traffic with inner VLAN tag 30 and outer VLAN tag 200.

```
[SwitchC] traffic classifier downlink_out
```

```
[SwitchC-classifier-downlink_out] if-match customer-vlan-id 30
```

```
[SwitchC-classifier-downlink_out] if-match service-vlan-id 200
```

```
[SwitchC-classifier-downlink_out] quit
```

# Configure a behavior named **downlink\_out** to change the inner VLAN tag into VLAN tag 10 and change the outer VLAN tag into VLAN tag 100.

```
[SwitchC] traffic behavior downlink_out
```

```
[SwitchC-behavior-downlink_out] remark customer-vlan-id 10
```

```
[SwitchC-behavior-downlink_out] remark service-vlan-id 100
```

```
[SwitchC-behavior-downlink_out] quit
```

# Create a QoS policy named **downlink\_out**.

```
[SwitchC] qos policy downlink_out
```

# Associate class **downlink\_out** with traffic behavior **downlink\_out** in the QoS policy.

```
[SwitchC-qospolicy-downlink_out] classifier downlink_out behavior downlink_out
```

```
[SwitchC-qospolicy-downlink_out] quit
```

# Apply QoS policy **downlink\_out** to the outgoing traffic of GigabitEthernet 1/0/1.

```
[SwitchC] interface GigabitEthernet 1/0/1
```

```
[SwitchC-GigabitEthernet1/0/1] qos apply policy downlink_out outbound
```

```
[SwitchC-GigabitEthernet1/0/1] quit
```

## Configuring Switch D

# Create VLAN 200.

```
<SwitchD> system-view
```

```
[SwitchD] vlan 200
```

```
[SwitchD-vlan200] quit
```

# Configure QinQ on GigabitEthernet 1/0/2 to add outer VLAN tag 200 to packets from VLAN 30.

```
[SwitchD] interface gigabitethernet 1/0/2
```

```
[SwitchD-GigabitEthernet1/0/2] port access vlan 200
```

```
[SwitchD-GigabitEthernet1/0/2] qinq enable
```

```
[SwitchD-GigabitEthernet1/0/2] quit
```

# Configure GigabitEthernet 1/0/1 as a trunk port.

```
[SwitchD] interface gigabitethernet 1/0/1
```

```
[SwitchD-GigabitEthernet1/0/1] port link-type trunk
```

# Assign GigabitEthernet 1/0/1 to VLAN 200.

```
[SwitchD-GigabitEthernet1/0/1] port trunk permit vlan 200
```

```
Remove GigabitEthernet 1/0/1 from VLAN 1.
[SwitchD-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchD-GigabitEthernet1/0/1] quit
```

## Verifying the configuration

# Display the port configurations. This example uses GigabitEthernet 1/0/1 on Switch C.

```
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1]display this
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 200
qos apply policy uplink_in inbound
qos apply policy downlink_out outbound
#
return
```

# Display the QoS policies applied to GigabitEthernet 1/0/1 of Switch C.

```
[SwitchC]display qos policy interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
```

```
Direction: Inbound
```

```
Policy: uplink_in
Classifier: uplink_in
Operator: AND
Rule(s) : If-match customer-vlan-id 10
 If-match service-vlan-id 100
Behavior: uplink_in
Marking:
 Remark Service VLAN ID 200
```

```
Direction: Outbound
```

```
Policy: downlink_out
Classifier: downlink_out
Operator: AND
Rule(s) : If-match customer-vlan-id 30
 If-match service-vlan-id 200
Behavior: downlink_out
Marking:
 Remark Customer VLAN ID 10
Marking:
 Remark Service VLAN ID 100
```

# Display the QoS policies applied to GigabitEthernet 1/0/2 of Switch C.

```
[SwitchC]display qos policy interface GigabitEthernet 1/0/2
```

```
Interface: GigabitEthernet1/0/2

Direction: Outbound

Policy: uplink_out
Classifier: uplink_out
 Operator: AND
 Rule(s) : If-match customer-vlan-id 10
 If-match service-vlan-id 200
Behavior: uplink_out
Marking:
 Remark Customer VLAN ID 30
```

## Configuration files

- Switch A:

```
#
vlan 100
#
interface GigabitEthernet1/0/1
 port access vlan 100
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
```
- Switch B:

```
#
vlan 100
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
 qinq enable
```
- Switch C:



```

#
vlan 200
#
traffic classifier uplink_in operator and
 if-match customer-vlan-id 10
 if-match service-vlan-id 100
traffic classifier uplink_out operator and
 if-match customer-vlan-id 10
 if-match service-vlan-id 200
traffic classifier downlink_out operator and
 if-match customer-vlan-id 30
 if-match service-vlan-id 200
#
traffic behavior uplink_in
 remark service-vlan-id 200
traffic behavior uplink_out
 remark customer-vlan-id 30
traffic behavior downlink_out
 remark customer-vlan-id 10
 remark service-vlan-id 100
#
qos policy uplink_in
 classifier uplink_in behavior uplink_in
qos policy uplink_out
 classifier uplink_out behavior uplink_out
qos policy downlink_out
 classifier downlink_out behavior downlink_out
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200
 qos apply policy uplink_in inbound
 qos apply policy downlink_out outbound
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200
 qos apply policy uplink_out outbound

```

- Switch D:

```

#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200

```

```

interface GigabitEthernet1/0/2
port access vlan 200
qinq enable
```

# IPv4-based VRRP configuration examples

This chapter provides IPv4-based VRRP configuration examples.

## Example: Configuring a single VRRP group

### Applicable product matrix

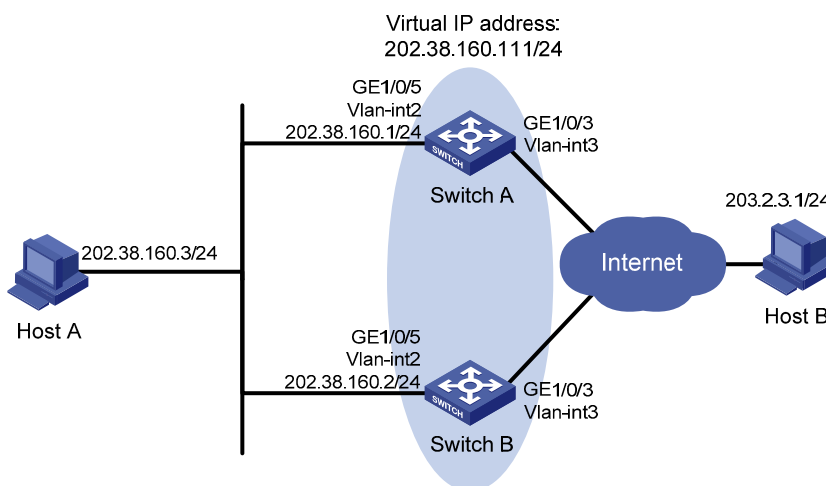
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

### Network requirements

As shown in [Figure 246](#), 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.
- When the uplink interface of Switch A fails, hosts can access the external network through Switch B.

**Figure 246 Network diagram**



## Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

For the hosts to access the external network when the uplink interface of Switch A fails, configure VRRP tracking on Switch A. When the uplink interface of Switch A is down or removed, Switch A decreases its priority and Switch B takes over to forward packets from the hosts.

To avoid frequent role change in the VRRP group, configure a preemption delay.

To enable the switches in the VRRP group to only process authorized packets, configure VRRP authentication.

## 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 allows a switch in the group to be elected as the master.

## Configuration procedures

### 1. Configure Switch A:

# Configure VLAN 3.

```
<SwitchA> system-view
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/3
[SwitchA-vlan3] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 100.0.0.2 24
[SwitchA-Vlan-interface3] quit
```

# Configure VLAN 2.

```
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
```

# Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 202.38.160.111/24.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

# Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

# Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

# Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

# Configure VRRP to monitor VLAN-interface 3 on Switch A. When the interface fails, the weight of Switch A decreases by 20 so Switch B can take over.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track interface vlan-interface 3 reduced 20
```

## 2. Configure Switch B:

# Configure VLAN 3.

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

```
[SwitchB] vlan 3
```

```
[SwitchB-vlan3] port gigabitethernet 1/0/3
```

```
[SwitchB-vlan3] quit
```

```
[SwitchB] interface vlan-interface 3
```

```
[SwitchB-Vlan-interface3] ip address 101.0.0.2 24
```

```
[SwitchB-Vlan-interface3] quit
```

# Configure VLAN 2.

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

```
[SwitchB] vlan 2
```

```
[SwitchB-Vlan2] port gigabitethernet 1/0/5
```

```
[SwitchB-Vlan2] quit
```

```
[SwitchB] interface vlan-interface 2
```

```
[SwitchB-Vlan-interface2] ip address 202.38.160.2 255.255.255.0
```

# Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 202.38.160.111/24.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

# Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

# Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

## 3. Configure Host A:

# Configure the default gateway of Host A as 202.38.160.111. (Details not shown.)

## Verifying the configuration

# Ping Host B from Host A. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
```

```
IPv4 Standby Information:
```

```

Run Mode : Standard
Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
VRID : 1 Adver Timer : 1
Admin Status : Up State : Master
Config Pri : 110 Running Pri : 110
Preempt Mode : Yes Delay Time : 5
Auth Type : Simple Key : *****
Virtual IP : 202.38.160.111
Virtual MAC : 0000-5e00-0101
Master IP : 202.38.160.1
VRRP Track Information:
Track Interface: Vlan3 State : Up Pri Reduced : 20

```

# Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
```

```

IPv4 Standby Information:
Run Mode : Standard
Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
VRID : 1 Adver Timer : 1
Admin Status : Up State : Backup
Config Pri : 100 Running Pri : 100
Preempt Mode : Yes Delay Time : 5
Become Master : 2200ms left
Auth Type : Simple Key : *****
Virtual IP : 202.38.160.111
Master IP : 202.38.160.1

```

The output shows that Switch A is operating as the master in VRRP group 1 to forward packets from Host A to Host B.

# Disconnect the link between Host A and Switch A, and verify that Host A can still ping Host B. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
```

```

IPv4 Standby Information:
Run Mode : Standard
Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
VRID : 1 Adver Timer : 1
Admin Status : Up State : Master
Config Pri : 100 Running Pri : 100
Preempt Mode : Yes Delay Time : 5
Auth Type : Simple Key : *****
Virtual IP : 202.38.160.111

```

```
Virtual MAC : 0000-5e00-0101
Master IP : 202.38.160.2
```

The output shows that when Switch A fails, Switch B takes over to forward packets from Host A to Host B.

# Recover the link between Host A and Switch A, and display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
 Run Mode : Standard
 Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
 VRID : 1 Adver Timer : 1
 Admin Status : Up State : Backup
 Config Pri : 110 Running Pri : 90
 Preempt Mode : Yes Delay Time : 5
 Become Master : 2200ms left
 Auth Type : Simple Key : *****
 Virtual IP : 202.38.160.111
 Master IP : 202.38.160.2
VRRP Track Information:
 Track Interface: Vlan3 State : Down Pri Reduced : 20
```

# Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
 Run Mode : Standard
 Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
 VRID : 1 Adver Timer : 1
 Admin Status : Up State : Master
 Config Pri : 100 Running Pri : 100
 Preempt Mode : Yes Delay Time : 5
 Auth Type : Simple Key : *****
 Virtual IP : 202.38.160.111
 Virtual MAC : 0000-5e00-0101
 Master IP : 202.38.160.2
```

The output shows that when VLAN-interface 3 on Switch A fails, the priority of Switch A decreases by 20. Switch A becomes the backup, and Switch B becomes the master to forward packets from Host A to Host B.

## Configuration files

Whether the authentication key is displayed in plain text or cipher text depends on the software version of the switch. This section displays a cipher-text authentication key.

- Switch A:

```

#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 202.38.160.1 255.255.255.0
 vrrp vrid 1 virtual-ip 202.38.160.111
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 track interface Vlan-interface3 reduced 20
 vrrp vrid 1 authentication-mode simple cipher c3$1FcANPYJckyfZyS7FA10cW8bBcUX
Nbbc
#
interface Vlan-interface3
 ip address 100.0.0.2 255.255.255.0
#
interface GigabitEthernet1/0/3
 port access vlan 3
#
interface GigabitEthernet1/0/5
 port access vlan 2
#

```

- Switch B:

```

#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 202.38.160.2 255.255.255.0
 vrrp vrid 1 virtual-ip 202.38.160.111
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 authentication-mode simple cipher c3$vxKRiU4Fy/p4dRTiw+znGTQyYNDfQrxb
#
interface Vlan-interface3
 ip address 101.0.0.2 255.255.255.0
#
interface GigabitEthernet1/0/3
 port access vlan 3
#
interface GigabitEthernet1/0/5
 port access vlan 2
#

```



# Example: Configuring VRRP-Track-NQA collaboration for the master to monitor the uplinks

## Applicable product matrix

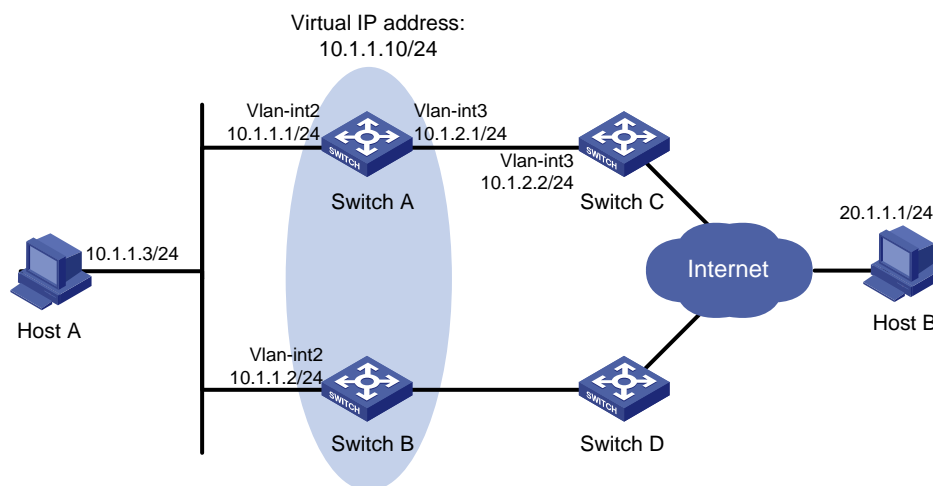
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

## Network requirements

As shown in [Figure 247](#), 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.
- When the uplink interface of Switch A fails, hosts can access the external network through Switch B.

**Figure 247 Network diagram**



## Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

For hosts to access the external network through Switch B when the uplink interface of Switch A fails, configure NQA to monitor the uplink of Switch A. When the uplink interface of Switch A fails, Switch A decreases its priority by a specific value.

To avoid frequent role change in the VRRP group, configure a preemption delay.

To enable the switches in the VRRP group to only process authorized packets, configure VRRP authentication.

## Configuration restrictions and guidelines

Configure the same virtual IP addresses, advertisement interval, and authentication method for each switch in the VRRP group. Make sure the number of virtual IP addresses assigned to them is also the same.

## Configuration procedures

1. Configure the IP address for each interface based on [Figure 247](#):

This example configures VLAN-interface 2 of Switch A. Configure other interfaces in the same way. (Details not shown.)

# Specify an IP address for VLAN-interface 2 on Switch A.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
[SwitchA-Vlan-interface2] quit
```

2. Create an NQA operation on Switch A:

# Create an NQA operation with administrator name **admin** and operation tag **test**.

```
[SwitchA] nqa entry admin test
```

# Specify the type of the NQA operation as **icmp-echo**.

```
[SwitchA-nqa-admin-test] type icmp-echo
```

# Configure the destination IP address of the ICMP echo operation as 10.1.2.2.

```
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.1.2.2
```

# Configure the ICMP echo operation to repeat at an interval of 100 milliseconds.

```
[SwitchA-nqa-admin-test-icmp-echo] frequency 100
```

# Create reaction entry 1. If the number of consecutive probe failures reaches 5, collaboration is triggered.

```
[SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail
threshold-type consecutive 5 action-type trigger-only
[SwitchA-nqa-admin-test-icmp-echo] quit
```

# Configure the scheduling parameters for the operation with the administrator name **admin** and operation tag **test**. The test starts now and lasts forever.

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

3. Configure a track entry on Switch A:

```
Create track entry 1, and associate it with reaction entry 1 of the NQA operation.
```

```
[SwitchA] track 1 nqa entry admin test reaction 1
```

4. Configure VRRP on Switch A:

```
Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 10.1.1.10.
```

```
[SwitchA] interface vlan-interface 2
```

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

```
Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.
```

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

```
Configure the authentication mode of the VRRP group as simple and authentication key as hello.
```

```
[SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

```
Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.
```

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

```
Associate VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the priority of the router in the VRRP group by 20 when the state of track entry 1 changes to negative.
```

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 reduced 20
```

5. Configure VRRP on Switch B:

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

```
[SwitchB] interface vlan-interface 2
```

```
Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 10.1.1.10.
```

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

```
Configure the authentication mode of the VRRP group as simple and authentication key as hello.
```

```
[SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

```
Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.
```

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

6. Configure Host A:

```
Configure the default gateway of Host A as 10.1.1.10. (Details not shown.)
```

## Verifying the configuration

```
Ping Host B from Host A. (Details not shown.)
```

```
Display detailed information about VRRP group 1 on Switch A.
```

```
[SwitchA-Vlan-interface2] display vrrp verbose
```

```
IPv4 Standby Information:
```

```
Run Mode : Standard
```

```
Run Method : Virtual MAC
```

```
Total number of virtual routers : 1
```

```
Interface Vlan-interface2
```

```
VRID : 1
```

```
Adver Timer : 1
```

```

Admin Status : Up State : Master
Config Pri : 110 Running Pri : 110
Preempt Mode : Yes Delay Time : 5
Auth Type : Simple Key : *****
Virtual IP : 10.1.1.10
Virtual MAC : 0000-5e00-0101
Master IP : 10.1.1.1

VRRP Track Information:
Track Object : 1 State : Positive Pri Reduced : 20

```

# Display detailed information about VRRP group 1 on Switch B.

```

[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
 Run Mode : Standard
 Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
 VRID : 1 Adver Timer : 1
 Admin Status : Up State : Backup
 Config Pri : 100 Running Pri : 100
 Preempt Mode : Yes Delay Time : 5
 Become Master : 2200ms left
 Auth Type : Simple Key : *****
 Virtual IP : 10.1.1.10
 Master IP : 10.1.1.1

```

The output shows that Switch A is operating as the master in VRRP group 1 to forward packets from Host A to Host B.

# Verify that Host A can still ping Host B. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.

```

[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
 Run Mode : Standard
 Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
 VRID : 1 Adver Timer : 1
 Admin Status : Up State : Backup
 Config Pri : 110 Running Pri : 90
 Preempt Mode : Yes Delay Time : 5
 Become Master : 2200ms left
 Auth Type : Simple Key : *****
 Virtual IP : 10.1.1.10
 Master IP : 10.1.1.2

VRRP Track Information:
Track Object : 1 State : Negative Pri Reduced : 20

```

# Display detailed information about VRRP group 1 on Switch B.

```

[SwitchB-Vlan-interface2] display vrrp verbose

```

```

IPv4 Standby Information:
 Run Mode : Standard
 Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
 VRID : 1 Adver Timer : 1
 Admin Status : Up State : Master
 Config Pri : 100 Running Pri : 100
 Preempt Mode : Yes Delay Time : 5
 Auth Type : Simple Key : *****
 Virtual IP : 10.1.1.10
 Virtual MAC : 0000-5e00-0101
 Master IP : 10.1.1.2

```

The output shows that when Switch A fails, the priority of Switch A decreases by 20. Switch A becomes the backup, and Switch B becomes the master to forward packets from Host A to Host B.

## Configuration files

Whether the authentication key is displayed in plain text or cipher text depends on the software version of the switch. This section displays a cipher-text authentication key.

- Switch A:

```

#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.10
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 track 1 reduced 20
 vrrp vrid 1 authentication-mode simple cipher c3$Fq7Gw6ux6gf6sjUnaPxfYaJSJ08r
xGhc
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
interface GigabitEthernet1/0/6
 port access vlan 3
#
nqa entry admin test
 type icmp-echo
 destination ip 10.1.2.2
 frequency 100

```

```

 reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
trigger-only
#
 track 1 nqa entry admin test reaction 1
#
 nqa schedule admin test start-time now lifetime forever
#

```

- Switch B:

```

#
vlan 2
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.10
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 authentication-mode simple cipher c3$1SjZTNgoayfie8IplIGd+p1lI64Q
oDs4
#
interface GigabitEthernet1/0/5
 port access vlan 2
#

```

## Example: Configuring VRRP-Track-BFD collaboration for the master to monitor the uplinks

### Applicable product matrix

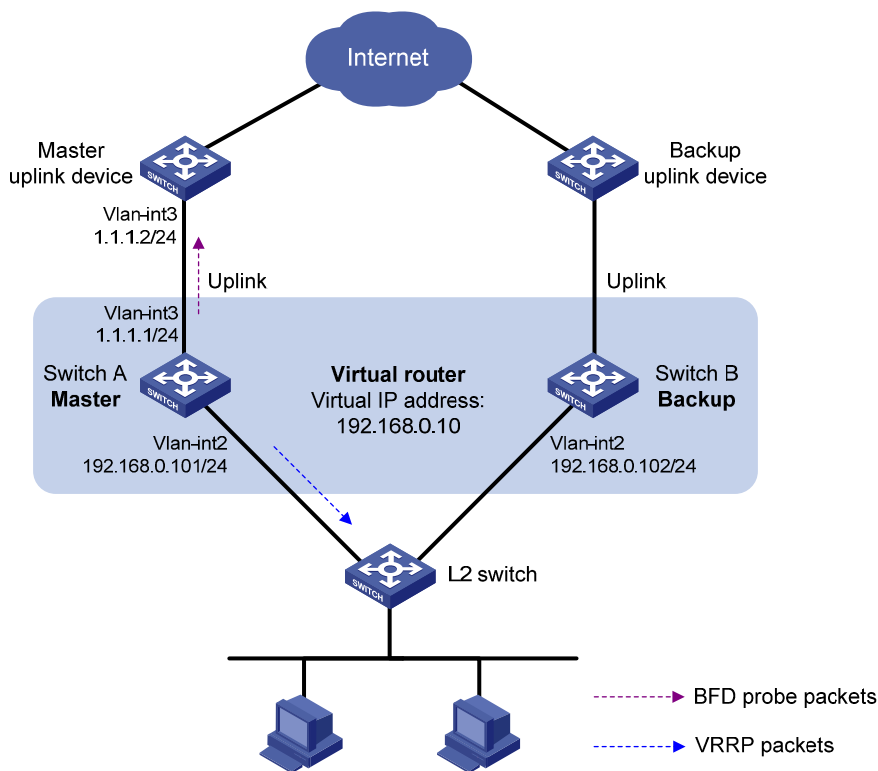
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

### Network requirements

As shown in [Figure 248](#), 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.
- When the uplink interface of Switch A fails, hosts can access the external network through Switch B.

Figure 248 Network diagram



## Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

For hosts to access the external network through Switch B when the uplink interface of Switch A fails, configure BFD to monitor the uplink of Switch A. When the uplink interface of Switch A fails, Switch A decreases its priority by a specific value.

To avoid frequent role change in the VRRP group, configure a preemption delay.

To enable the switches in the VRRP group to only process authorized packets, configure VRRP authentication.

## Configuration restrictions and guidelines

When you configure VRRP-Track-BFD collaboration, follow these restrictions and guidelines:

- Make sure the uplink device of the master supports BFD.
- Configure the same virtual IP addresses, advertisement interval, and authentication method for each switch in the VRRP group. Make sure the number of virtual IP addresses assigned to 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 248](#):

This example configures VLAN-interface 2 of Switch A. Configure other interfaces in the same way. (Details not shown.)

# Specify an IP address for VLAN-interface 2 on Switch A.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 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, which uses BFD 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:

# Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to **192.168.0.10**.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
```

# Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

# Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

# Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

# Associate VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the priority of Switch A in the VRRP group by 20 when the state of track entry 1 changes to negative.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 reduced 20
[SwitchA-Vlan-interface2] return
```

5. Configure VRRP on Switch B:

# Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 192.168.0.10.



```

<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
Configure the authentication mode of the VRRP group as simple and authentication key as hello.
[SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
[SwitchB-Vlan-interface2] return

```

## 6. Configure Host A:

Configure the default gateway of Host A as 192.168.0.10. (Details not shown.)

## Verifying the configuration

# Display detailed information about VRRP group 1 on Switch A.

```

<SwitchA> display vrrp verbose
IPv4 Standby Information:
 Run Mode : Standard
 Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
 VRID : 1 Adver Timer : 1
 Admin Status : Up State : Master
 Config Pri : 110 Running Pri : 110
 Preempt Mode : Yes Delay Time : 5
 Auth Type : Simple Key : *****
 Virtual IP : 192.168.0.10
 Virtual MAC : 0000-5e00-0101
 Master IP : 192.168.0.101
VRRP Track Information:
 Track Object : 1 State : Positive Pri Reduced : 20

```

# Display detailed information about track entry 1 on Switch A.

```

<SwitchA> display track 1
Track ID: 1
 Status: Positive
 Duration: 0 days 0 hours 0 minutes 7 seconds
 Notification delay: Positive 0, Negative 0 (in seconds)
 Reference object:
 BFD session:
 Packet type: Echo
 Interface : Vlan-interface3
 Remote IP : 1.1.1.2
 Local IP : 1.1.1.1

```

# Display detailed information about VRRP group 1 on Switch B.

```

<SwitchB> display vrrp verbose
IPv4 Standby Information:

```

```

Run Mode : Standard
Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
VRID : 1 Adver Timer : 1
Admin Status : Up State : Backup
Config Pri : 100 Running Pri : 100
Preempt Mode : Yes Delay Time : 5
Become Master : 2200ms left
Auth Type : Simple Key : *****
Virtual IP : 192.168.0.10
Master IP : 192.168.0.101

```

The output shows that when the status of track entry 1 becomes **Positive**, Switch A is the master, and Switch B the backup.

# When the uplink of Switch A goes down, the status of track entry 1 becomes **Negative**.

```

<SwitchA> display track 1
Track ID: 1
 Status: Negative
 Duration: 0 days 0 hours 0 minutes 20 seconds
 Notification delay: Positive 0, Negative 0 (in seconds)
 Reference object:
 BFD session:
 Packet type: Echo
 Interface : Vlan-interface3
 Remote IP : 1.1.1.2
 Local IP : 1.1.1.1

```

# Display detailed information about VRRP group 1 on Switch A.

```

<SwitchA> display vrrp verbose
IPv4 Standby Information:
 Run Mode : Standard
 Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
VRID : 1 Adver Timer : 1
Admin Status : Up State : Backup
Config Pri : 110 Running Pri : 90
Preempt Mode : Yes Delay Time : 5
Become Master : 2200ms left
Auth Type : Simple Key : *****
Virtual IP : 192.168.0.10
Master IP : 192.168.0.102
VRRP Track Information:
 Track Object : 1 State : Negative Pri Reduced : 20

```

# Display detailed information about VRRP group 1 on Switch B.

```

<SwitchB> display vrrp verbose
IPv4 Standby Information:

```

```

Run Mode : Standard
Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
VRID : 1 Adver Timer : 1
Admin Status : Up State : Master
Config Pri : 100 Running Pri : 100
Preempt Mode : Yes Delay Time : 5
Become Master : 2200ms left
Auth Type : Simple Key : *****
Virtual IP : 192.168.0.10
Virtual MAC : 0000-5e00-0101
Master IP : 192.168.0.102

```

The output shows that when Switch A detects that the uplink fails through BFD, it decreases its priority to 90 to make sure Switch B can become the master.

## Configuration files

Whether the authentication key is displayed in plain text or cipher text depends on the software version of the switch. This section displays a cipher-text authentication key.

- Switch A:

```

#
bfd echo-source-ip 10.10.10.10
#
vlan 2 to 3
#
interface Vlan-interface2
ip address 192.168.0.101 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.0.10
vrrp vrid 1 priority 110
vrrp vrid 1 preempt-mode timer delay 5
vrrp vrid 1 track 1 reduced 20
vrrp vrid 1 authentication-mode simple cipher c3$8j5zt3i82EKmOjERTrq8BiL906Sv
iDVp
#
interface Vlan-interface3
ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/5
port access vlan 2
#
interface GigabitEthernet1/0/6
port access vlan 3
#
track 1 bfd echo interface Vlan-interface3 remote ip 1.1.1.2 local ip 1.1.1.1
#

```

- Switch B:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.0.102 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.0.10
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 authentication-mode simple cipher c3$1SjZTNgoayfie8IplIGd+p11I64Q
oDs4
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
```

## Example: Configuring VRRP-Track-BFD collaboration for a backup to monitor the master

### Applicable product matrix

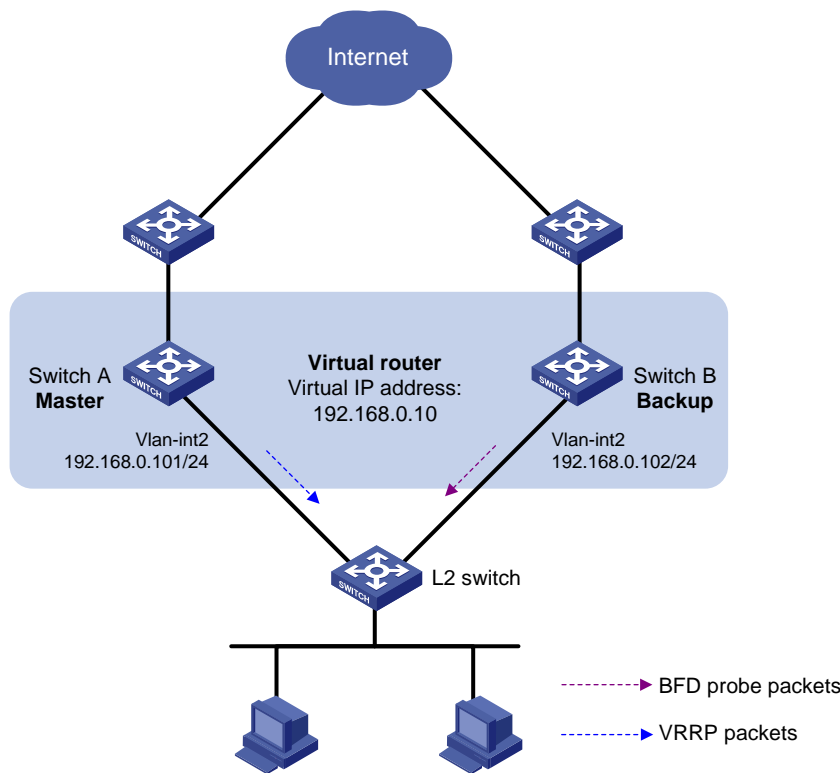
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

### Network requirements

As shown in [Figure 249](#), 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.
- When the uplink interface of Switch A fails, hosts can access the external network through Switch B.

Figure 249 Network diagram



## Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

To avoid frequent role change in the VRRP group, configure a preemption delay.

To enable the switches in the VRRP group to only process authorized packets, configure VRRP authentication.

## Configuration restrictions and guidelines

When you configure BFD for a VRRP backup to monitor the master, follow these restrictions and guidelines:

- Configure the same virtual IP addresses, advertisement interval, and authentication method for each switch in the VRRP group. Make sure the number of virtual IP addresses assigned to 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 249](#):

This example configures VLAN-interface 2 of Switch A. Configure other interfaces in the same way. (Details not shown.)

# Configure Switch A:

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.0.101 255.255.255.0
```

2. Configure VRRP on Switch A:

# Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to **192.168.0.10**.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
```

# Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

# Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

# Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
[SwitchA-Vlan-interface2] return
```

3. Configure BFD on Switch B:

# Specify the source IP address for BFD echo packets as **10.10.10.10**.

```
<SwitchB> system-view
[SwitchB] bfd echo-source-ip 10.10.10.10
```

4. Configure a track entry on Switch B:

# Create track entry 1, which uses BFD to monitor the link between local IP address 192.168.0.102 and remote IP address 192.168.0.101 by sending BFD echo packets

```
[SwitchB] track 1 bfd echo interface vlan-interface 2 remote ip 192.168.0.101 local ip 192.168.0.102
```

5. Configure VRRP on Switch B:

# Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to **192.168.0.10**.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
```

# Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

# Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

# Configure VRRP group 1 to monitor the status of track entry 1. When the status of the track entry becomes Negative, Switch B quickly becomes the master.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 track 1 switchover
[SwitchB-Vlan-interface2] return
```

## 6. Configure the hosts:

# Configure the default gateway of the hosts as **192.168.0.10**. (Details not shown.)

## Verifying the configuration

# Display detailed information about VRRP group 1 on Switch A.

```
<SwitchA> display vrrp verbose
IPv4 Standby Information:
 Run Mode : Standard
 Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
 VRID : 1
 Admin Status : Up
 Config Pri : 110
 Preempt Mode : Yes
 Auth Type : Simple
 Virtual IP : 192.168.0.10
 Virtual MAC : 0000-5e00-0101
 Master IP : 192.168.0.101
 Adver Timer : 1
 State : Master
 Running Pri : 110
 Delay Time : 5
 Key : *****
```

# Display detailed information about VRRP group 1 on Switch B.

```
<SwitchB> display vrrp verbose
IPv4 Standby Information:
 Run Mode : Standard
 Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
 VRID : 1
 Admin Status : Up
 Config Pri : 100
 Preempt Mode : Yes
 Become Master : 2200ms left
 Auth Type : Simple
 Virtual IP : 192.168.0.10
 Master IP : 192.168.0.101
 Adver Timer : 1
 State : Backup
 Running Pri : 100
 Delay Time : 5
 Key : *****
VRRP Track Information:
 Track Object : 1
 State : Positive
 Switchover
```

# Display information about track entry 1 on Switch B.

```
<SwitchB> display track 1
Track ID: 1
 Status: Positive
 Duration: 0 days 0 hours 2 minutes 22 seconds
```

```

Notification delay: Positive 0, Negative 0 (in seconds)
Reference object:
 BFD session:
 Packet type: Echo
 Interface : Vlan-interface2
 Remote IP : 192.168.0.101
 Local IP : 192.168.0.102

```

The output shows that when the status of the track entry becomes Positive, Switch A is the master and Switch B the backup.

# Enable VRRP state debugging and BFD event debugging on Switch B.

```

<SwitchB> terminal debugging
<SwitchB> terminal monitor
<SwitchB> debugging vrrp state
<SwitchB> debugging bfd event

```

# When Switch A or its uplink interface fails, the following output is displayed on Switch B.

```

*Dec 17 14:44:34:142 2012 SwitchB BFD/7/EVENT: Send sess-down Msg,
[Src:192.168.0.102,Dst:192.168.0.101,Vlan-interface2,Echo], instance:0, protocol:Track
*Dec 17 14:44:34:144 2012 SwitchB VRRP/7/DebugState: IPv4 Vlan-interface2 | Virtual Router
1 : Backup --> Master reason: The status of the tracked object changed

```

# Display detailed information about VRRP group 1 on Switch B.

```

<SwitchB> display vrrp verbose
IPv4 Standby Information:
 Run Mode : Standard
 Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
 VRID : 1 Adver Timer : 1
 Admin Status : Up State : Master
 Config Pri : 100 Running Pri : 100
 Preempt Mode : Yes Delay Time : 5
 Auth Type : Simple Key : *****
 Virtual IP : 192.168.0.10
 Virtual MAC : 0000-5e00-0101
 Master IP : 192.168.0.102
VRRP Track Information:
 Track Object : 1 State : Negative Switchover

```

The output shows that when BFD detects that Switch A fails, 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 vrid 1 virtual-ip 192.168.0.10
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 authentication-mode simple cipher c3$Fq7Gw6ux6gf6sjUnaPxfYaJSJ08r
xGhc
#
interface GigabitEthernet1/0/5
 port access vlan 2
#

```

- Switch B:

```

#
 bfd echo-source-ip 10.10.10.10
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.0.102 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.0.10
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 track 1 switchover
 vrrp vrid 1 authentication-mode simple cipher c3$1SjZTNGoayfie8IplIGd+p11I64Q
oDs4
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
track 1 bfd echo interface vlan-interface 2 remote ip 192.168.0.101 local ip
192.168.0.102
#

```

## Example: Configuring multiple VRRP groups

### Applicable product matrix

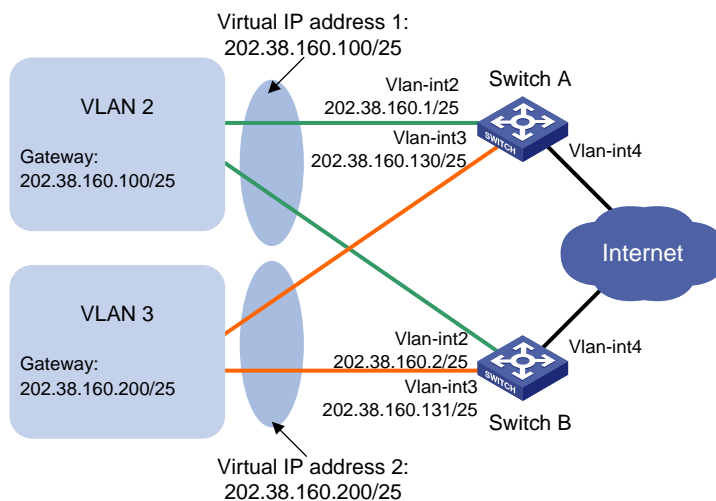
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

## Network requirements

As shown in [Figure 250](#), Switch A and Switch B form two VRRP groups. Implement the following requirements:

- Switch A operates as the master of VRRP group 1 to forward packets from VLAN 2, and Switch B operates as the master of VRRP group 2 to forward packets from VLAN3. When one of the switches fails, the other switch provides gateway service for both areas.
- When the uplink interface of one switch fails, hosts can access the external network through the other switch.

**Figure 250 Network diagram**



## Requirements analysis

For the hosts to access the external network when the uplink interface of the master in a VRRP group fails, configure VRRP tracking on the master. When the uplink interface of the master fails, the master decreases its priority and the backup takes over to forward packets from the hosts.

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

To avoid frequent role change in the VRRP group, configure a preemption delay.

## Configuration restrictions and guidelines

Configure the same virtual IP addresses, advertisement interval, and authentication method for each switch in one VRRP group. Make sure the number of virtual IP addresses assigned to them is also the same.

You can configure collation between VRRP and Track, NQA, or BFD on the master to monitor the uplink status. For more information, see "[Example: Configuring VRRP-Track-NQA collaboration for the master to monitor the uplinks.](#)"

You can configure BFD for a VRRP backup to monitor the master. For more information, see "[Example: Configuring VRRP-Track-BFD collaboration for a backup to monitor the master.](#)"

## Configuration procedures

### 1. Configure Switch A:

#### # Configure VLAN 4.

```
<SwitchA> system-view
[SwitchA] vlan 4
[SwitchA-vlan4] port gigabitethernet 1/0/7
[SwitchA-vlan4] quit
[SwitchA] interface vlan-interface 4
[SwitchA-Vlan-interface4] ip address 20.1.1.2 255.255.255.0
[SwitchA-Vlan-interface4] quit
```

#### # Configure VLAN 2.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 202.38.160.1 255.255.255.128
```

#### # Create VRRP group 1, and set its virtual IP address to **202.38.160.100**.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.100
```

#### # Assign Switch A a priority of 110 in VRRP group 1.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

#### # Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

#### # On VLAN-interface 2, configure the interface to be tracked as VLAN-interface 4. The priority of Switch A will decrement by 30 when VLAN-interface 4 is down.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track interface vlan-interface 4 reduced 30
[SwitchA-Vlan-interface2] quit
```

#### # Configure VLAN 3.

```
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/6
[SwitchA-vlan3] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 202.38.160.130 255.255.255.128
```

#### # Create VRRP group 2, and set its virtual IP address to **202.38.160.200**.

```
[SwitchA-Vlan-interface3] vrrp vrid 2 virtual-ip 202.38.160.200
```

#### # Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchA-Vlan-interface3] vrrp vrid 2 preempt-mode timer delay 5
```

## 2. Configure Switch B:

### # Configure VLAN 4.

```
<SwitchB> system-view
[SwitchB] vlan 4
[SwitchB-vlan4] port gigabitethernet 1/0/7
[SwitchB-vlan4] quit
[SwitchB] interface vlan-interface 4
[SwitchB-Vlan-interface4] ip address 30.1.1.2 255.255.255.0
[SwitchB-Vlan-interface4] quit
```

### # Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 202.38.160.2 255.255.255.128
```

### # Create VRRP group 1, and set its virtual IP address to **202.38.160.100**.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.100
```

### # Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
[SwitchB-Vlan-interface2] quit
```

### # Configure VLAN 3.

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/6
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 202.38.160.131 255.255.255.128
```

### # Create VRRP group 2, and set its virtual IP address to **202.38.160.200**.

```
[SwitchB-Vlan-interface3] vrrp vrid 2 virtual-ip 202.38.160.200
```

### # Assign Switch B a priority of 110 in VRRP group 2.

```
[SwitchB-Vlan-interface3] vrrp vrid 2 priority 110
```

### # Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchB-Vlan-interface3] vrrp vrid 2 preempt-mode timer delay 5
```

### # On VLAN-interface 3, configure the interface to be tracked as VLAN-interface 4. The priority of Switch B will decrement by 30 when VLAN-interface 4 is down.

```
[SwitchB-Vlan-interface3] vrrp vrid 2 track interface vlan-interface 4 reduced 30
```

## 3. Configure the hosts:

# Configure the default gateway of the hosts in VLAN 2 as **202.38.160.100/25** and in VLAN 3 as **202.38.160.200/25**. (Details not shown.)

## Verifying the configuration

# Display detailed information about the VRRP groups on Switch A.

```
[SwitchA-Vlan-interface3] display vrrp verbose
IPv4 Standby Information:
 Run Mode : Standard
 Run Method : Virtual MAC
Total number of virtual routers : 2
Interface Vlan-interface2
 VRID : 1 Adver Timer : 1
 Admin Status : Up State : Master
 Config Pri : 110 Running Pri : 110
 Preempt Mode : Yes Delay Time : 5
 Auth Type : None
 Virtual IP : 202.38.160.100
 Virtual MAC : 0000-5e00-011e
 Master IP : 202.38.160.1
VRRP Track Information:
Track Interface: Vlan4 State : Up Pri Reduced : 30

Interface Vlan-interface3
 VRID : 2 Adver Timer : 1
 Admin Status : Up State : Backup
 Config Pri : 100 Running Pri : 100
 Preempt Mode : Yes Delay Time : 5
 Become Master : 2200ms left
 Auth Type : None
 Virtual IP : 202.38.160.200
 Master IP : 202.38.160.131
```

# Display detailed information about the VRRP groups on Switch B.

```
[SwitchB-Vlan-interface3] display vrrp verbose
IPv4 Standby Information:
 Run Mode : Standard
 Run Method : Virtual MAC
Total number of virtual routers : 2
Interface Vlan-interface2
 VRID : 1 Adver Timer : 1
 Admin Status : Up State : Backup
 Config Pri : 100 Running Pri : 100
 Preempt Mode : Yes Delay Time : 5
 Become Master : 2200ms left
 Auth Type : None
 Virtual IP : 202.38.160.100
 Master IP : 202.38.160.1

Interface Vlan-interface3
 VRID : 2 Adver Timer : 1
```

```

Admin Status : Up State : Master
Config Pri : 110 Running Pri : 110
Preempt Mode : Yes Delay Time : 5
Auth Type : None
Virtual IP : 202.38.160.200
Virtual MAC : 0000-5e00-0120
Master IP : 202.38.160.131
VRRP Track Information:
Track Interface: Vlan4 State : Up Pri Reduced : 30

```

The output shows 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 group 1 on Switch B when Switch A fails.

```
[SwitchB-Vlan-interface3] display vrrp verbose
```

```
IPv4 Standby Information:
```

```

Run Mode : Standard
Run Method : Virtual MAC

```

```
Total number of virtual routers : 2
```

```
Interface Vlan-interface2
```

```

VRID : 1 Adver Timer : 1
Admin Status : Up State : Master
Config Pri : 100 Running Pri : 100
Preempt Mode : Yes Delay Time : 5
Auth Type : None
Virtual IP : 202.38.160.100
Virtual MAC : 0000-5e00-011e
Master IP : 202.38.160.2

```

```
Interface Vlan-interface3
```

```

VRID : 2 Adver Timer : 1
Admin Status : Up State : Master
Config Pri : 110 Running Pri : 110
Preempt Mode : Yes Delay Time : 5
Auth Type : None
Virtual IP : 202.38.160.200
Virtual MAC : 0000-5e00-0120
Master IP : 202.38.160.131

```

```
VRRP Track Information:
```

```
Track Interface: Vlan4 State : Up Pri Reduced : 30
```

The output shows that when Switch A fails, Switch B operates as the master in VRRP group 1 to forward Internet traffic for hosts in VLAN 2.

# Configuration files

- Switch A:

```
#
vlan 2 to 4
#
interface Vlan-interface2
 ip address 202.38.160.1 255.255.255.128
 vrrp vrid 1 virtual-ip 202.38.160.100
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 track interface Vlan-interface4 reduced 30
#
interface Vlan-interface3
 ip address 202.38.160.130 255.255.255.128
 vrrp vrid 2 virtual-ip 202.38.160.200
 vrrp vrid 2 preempt-mode timer delay 5
#
interface Vlan-interface4
 ip address 20.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
interface GigabitEthernet1/0/6
 port access vlan 3
#
interface GigabitEthernet1/0/7
 port access vlan 4
#
```

- Switch B:

```
#
vlan 2 to 4
#
interface Vlan-interface2
 ip address 202.38.160.2 255.255.255.128
 vrrp vrid 1 virtual-ip 202.38.160.100
 vrrp vrid 1 preempt-mode timer delay 5
#
interface Vlan-interface3
 ip address 202.38.160.131 255.255.255.128
 vrrp vrid 2 virtual-ip 202.38.160.200
 vrrp vrid 2 priority 110
 vrrp vrid 2 preempt-mode timer delay 5
 vrrp vrid 2 track interface Vlan-interface4 reduced 30
#
interface Vlan-interface4
```

```
ip address 30.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/5
port access vlan 2
#
interface GigabitEthernet1/0/6
port access vlan 3
#
interface GigabitEthernet1/0/7
port access vlan 4
#
```

## Example: Using VRRP with MSTP

### Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

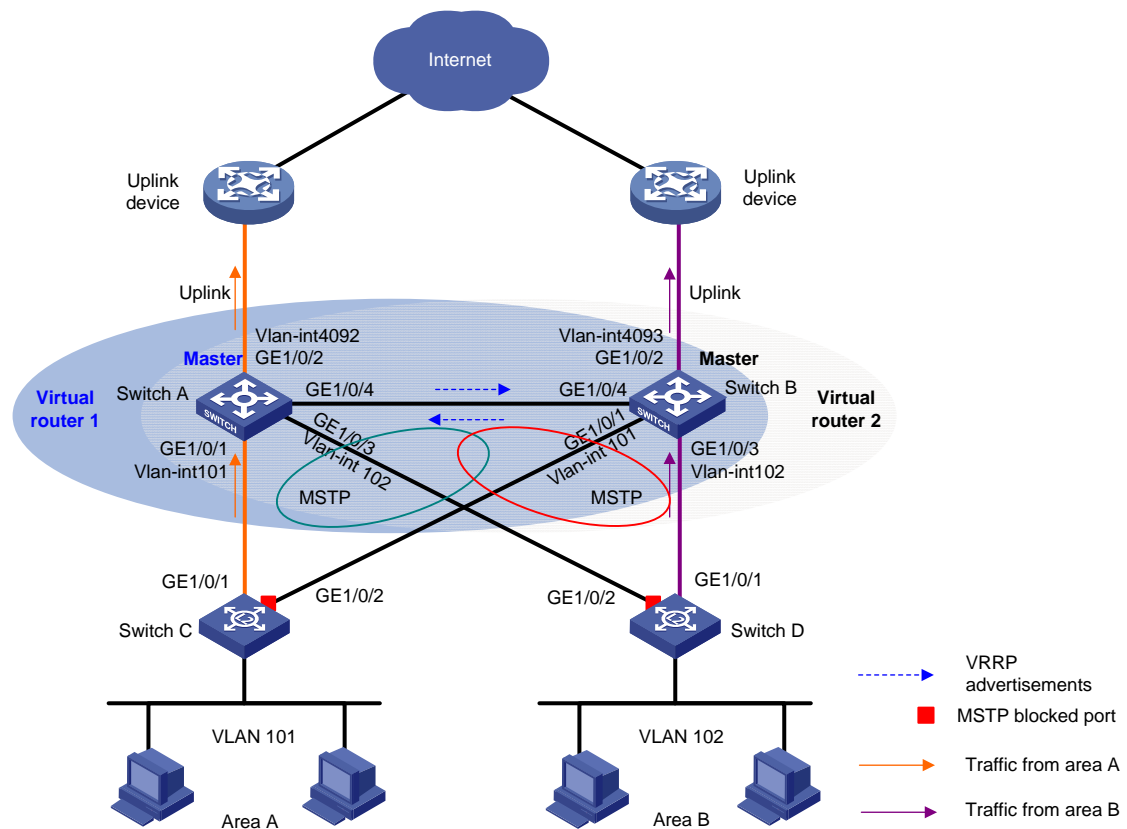
### Network requirements

As shown in [Figure 251](#), Switch A and Switch B form two VRRP groups. Implement the following requirements:

- Switch A operates as the master of VRRP group 1 to forward packets from VLAN 2, and Switch B operates as the master of VRRP group 2 to forward packets from VLAN3. When one of the switches fails, the other switch provides gateway service for both VLANs.
- When the uplink interface of one switch fails, hosts can access the external network through the other switch.



Figure 251 Network diagram



## Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

For the hosts to access the external network when the uplink interface of the master in a VRRP group fails, configure VRRP tracking on the master. When the uplink interface of the master is down or removed, the master decreases its priority and the backup takes over to forward packets from the hosts.

To avoid loops between Switch A, Switch B, Switch C, and Switch D, enable MSTP on them.

## Configuration procedures

### 1. Configure Switch A:

# Assign GigabitEthernet 1/0/1 to VLAN 101, GigabitEthernet 1/0/3 to VLAN 102, and GigabitEthernet 1/0/2 to VLAN 4092.

```
<SwitchA> system-view
[SwitchA] vlan 101
[SwitchA-vlan101] port gigabitethernet 1/0/1
[SwitchA-vlan101] quit
[SwitchA] vlan 102
[SwitchA-vlan102] port gigabitethernet 1/0/3
```

```

[SwitchA-vlan102] quit
[SwitchA] vlan 4092
[SwitchA-vlan4092] port gigabitethernet 1/0/2
[SwitchA-vlan4092] quit

Configure the link type of GigabitEthernet 1/0/4 as trunk, and assign GigabitEthernet 1/0/4
to VLAN 101 and VLAN 102.

[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-type trunk
[SwitchA-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[SwitchA-GigabitEthernet1/0/4] port trunk permit vlan 101 to 102
[SwitchA-GigabitEthernet1/0/4] port trunk pvid vlan 101
[SwitchA-GigabitEthernet1/0/4] quit

Configure the uplink interface.

[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] undo stp enable
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface vlan-interface 4092
[SwitchA-Vlan-interface4092] ip address 10.1.1.2 24

Create VRRP group 1 and assign virtual IP address 10.10.101.1 to the VRRP group, and
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 interface vlan-interface 4092 reduced
20
[SwitchA-Vlan-interface101] quit

Create VRRP group 2.

[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] ip address 10.10.102.2 24
[SwitchA-Vlan-interface102] vrrp vrid 1 virtual-ip 10.10.102.1
[SwitchA-Vlan-interface102] quit

Configure MSTP.

[SwitchA] stp region-configuration
[SwitchA-mst-region] region-name vrrp
[SwitchA-mst-region] instance 1 vlan 101
[SwitchA-mst-region] instance 2 vlan 102
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
[SwitchA] stp instance 1 root primary
[SwitchA] stp instance 2 root secondary
[SwitchA] stp enable

```

## 2. Configure Switch B:

# Assign GigabitEthernet 1/0/1 to VLAN 101, GigabitEthernet 1/0/3 to VLAN 102, and GigabitEthernet 1/0/2 to VLAN 4093.

```
<SwitchB> system-view
[SwitchB] vlan 101
[SwitchB-vlan101] port gigabitethernet 1/0/1
[SwitchB-vlan101] quit
[SwitchB] vlan 102
[SwitchB-vlan102] port gigabitethernet 1/0/3
[SwitchB-vlan102] quit
[SwitchB] vlan 4093
[SwitchB-vlan4093] port gigabitethernet 1/0/2
[SwitchB-vlan4093] quit
```

# Configure the link type of GigabitEthernet 1/0/4 as trunk, and assign GigabitEthernet 1/0/4 to VLAN 101 and VLAN 102.

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] port link-type trunk
[SwitchB-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[SwitchB-GigabitEthernet1/0/4] port trunk permit vlan 101 to 102
[SwitchB-GigabitEthernet1/0/4] port trunk pvid vlan 101
[SwitchB-GigabitEthernet1/0/4] quit
```

# Configure the uplink interface.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] undo stp enable
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface vlan-interface 4093
[SwitchB-Vlan-interface4093] ip address 10.1.2.2 24
```

# Create VRRP group 1.

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ip address 10.10.101.3 24
[SwitchB-Vlan-interface101] vrrp vrid 1 virtual-ip 10.10.101.1
[SwitchB-Vlan-interface101] quit
```

# Create VRRP group 2 and assign virtual IP address **10.10.102.1** to the VRRP group, and 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 interface vlan-interface 4093 reduced 20
[SwitchB-Vlan-interface102] quit
```

# Configure MSTP.

```
[SwitchB] stp region-configuration
```

```
[SwitchB-mst-region] region-name vrrp
[SwitchB-mst-region] instance 1 vlan 101
[SwitchB-mst-region] instance 2 vlan 102
[SwitchB-mst-region] active region-configuration
[SwitchB-mst-region] quit
[SwitchB] stp instance 2 root primary
[SwitchB] stp instance 1 root secondary
[SwitchB] stp enable
```

### 3. Configure Switch C:

# Configure VLAN 101.

```
<SwitchC> system-view
[SwitchC] vlan 101
[SwitchC-vlan101] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[SwitchC-vlan101] quit
```

# Configure MSTP.

```
[SwitchC] stp region-configuration
[SwitchC-mst-region] region-name vrrp
[SwitchC-mst-region] instance 1 vlan 101
[SwitchC-mst-region] instance 2 vlan 102
[SwitchC-mst-region] active region-configuration
[SwitchC-mst-region] quit
[SwitchC] stp enable
```

### 4. Configure Switch D:

# Configure VLAN 102.

```
<SwitchD> system-view
[SwitchD] vlan 102
[SwitchD-vlan102] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[SwitchD-vlan102] quit
```

# Configure MSTP.

```
[SwitchD] stp region-configuration
[SwitchD-mst-region] region-name vrrp
[SwitchD-mst-region] instance 1 vlan 101
[SwitchD-mst-region] instance 2 vlan 102
[SwitchD-mst-region] active region-configuration
[SwitchD-mst-region] quit
[SwitchD] stp enable
```

### 5. Configure the hosts:

# Configure the default gateway 10.10.101.1 for hosts in area A and 10.10.102.1 for hosts in a area B. (Details not shown.)

## Verifying the configuration

Execute the **display vrrp verbose** command to display detailed information about the VRRP group. Execute the **display stp brief** command to display brief information about MSTP.

# Configuration files

- Switch A:

```
#
vlan 101 to 102
#
vlan 4092
#
stp region-configuration
region-name vrrp
instance 1 vlan 101
instance 2 vlan 102
active region-configuration
#
stp instance 1 root primary
stp instance 2 root secondary
stp enable
#
interface Vlan-interface101
ip address 10.10.101.2 255.255.255.0
vrrp vrid 1 virtual-ip 10.10.101.1
vrrp vrid 1 priority 110
vrrp vrid 1 track interface Vlan-interface4092 reduced 20
#
interface Vlan-interface102
ip address 10.10.102.2 255.255.255.0
vrrp vrid 1 virtual-ip 10.10.102.1
#
interface Vlan-interface4092
ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port access vlan 101
#
interface GigabitEthernet1/0/2
port access vlan 4092
#
interface GigabitEthernet1/0/3
port access vlan 102
#
interface GigabitEthernet1/0/4
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 101 to 102
port trunk pvid vlan 101
#
```

- Switch B:

```

#
vlan 101 to 102
#
vlan 4093
#
stp region-configuration
region-name vrrp
instance 1 vlan 101
instance 2 vlan 102
active region-configuration
#
stp instance 1 root secondary
stp instance 2 root primary
stp enable
#
interface Vlan-interface101
ip address 10.10.101.3 255.255.255.0
vrrp vrid 1 virtual-ip 10.10.101.1
#
interface Vlan-interface102
ip address 10.10.102.3 255.255.255.0
vrrp vrid 1 virtual-ip 10.10.102.1
vrrp vrid 1 priority 110
vrrp vrid 1 track interface Vlan-interface4093 reduced 20
#
interface Vlan-interface4093
ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port access vlan 101
#
interface GigabitEthernet1/0/2
port access vlan 4093
#
interface GigabitEthernet1/0/3
port access vlan 102
#
interface GigabitEthernet1/0/4
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 101 to 102
port trunk pvid vlan 101
#

```

- Switch C:

```

#
vlan 101
#
stp region-configuration

```

```

region-name vrrp
instance 1 vlan 101
instance 2 vlan 102
active region-configuration
#
stp enable
#
interface GigabitEthernet1/0/1
port access vlan 101
#
interface GigabitEthernet1/0/2
port access vlan 101
#

```

- Switch D:

```

#
vlan 102
#
stp region-configuration
region-name vrrp
instance 1 vlan 101
instance 2 vlan 102
active region-configuration
#
stp enable
#
interface GigabitEthernet1/0/1
port access vlan 102
#
interface GigabitEthernet1/0/2
port access vlan 102
#

```

## Example: Configuring VRRP load balancing mode

### Applicable product matrix

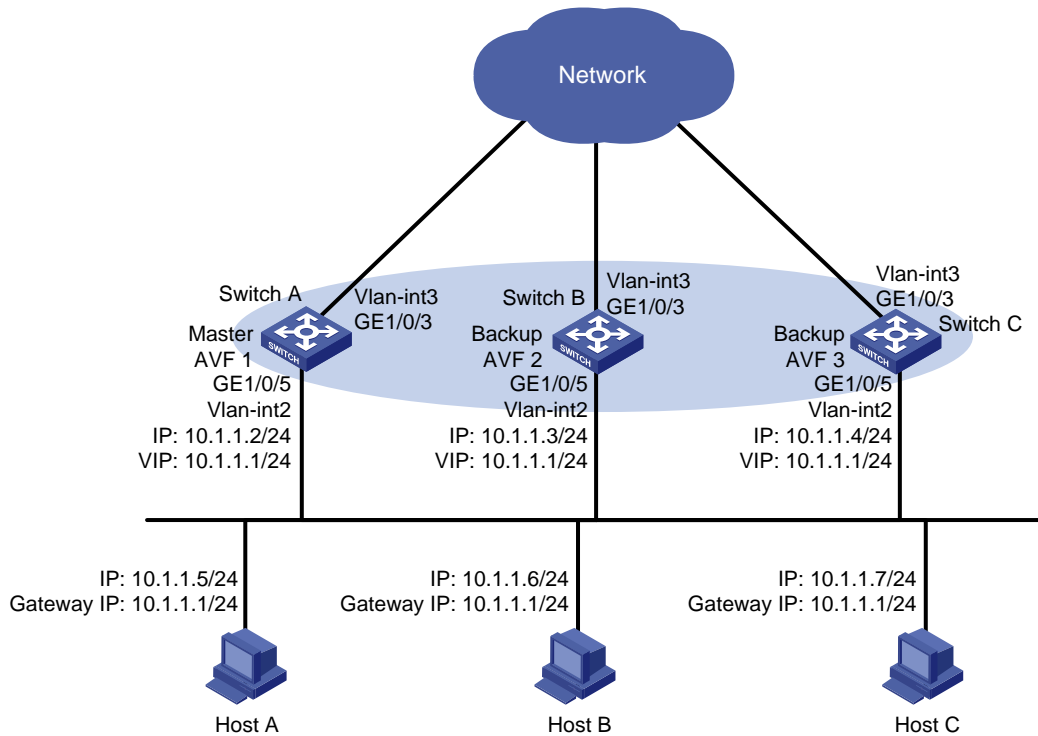
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

### Network requirements

As shown in [Figure 252](#), Switch A, Switch B, and Switch C form a load-balanced VRRP group and use the virtual IP address 10.1.1.1/24 to provide gateway service. Implement 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.
- When the upstream link of the active virtual forwarder (AVF) fails, the AVF can notify a listening virtual forwarder (LVF) to take over.

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.

## 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. It cannot be 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. For an LVF to become the AVF when the upstream link of the VF owner fails, the reduced weight for the VF owner must be higher than 245.



- 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 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> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port 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 timer delay 5
[SwitchA-Vlan-interface2] quit
```

# Create track entry 1 and associate it with the link state of VLAN-interface 3.

```
[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 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> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port 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 timer delay 5
[SwitchB-Vlan-interface2] quit
```

# Create track entry 1 and associate it with the link state of VLAN-interface 3.

```
[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 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> system-view
[SwitchC] vlan 2
[SwitchC-vlan2] port 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 timer delay 5
[SwitchC-Vlan-interface2] quit
Create track entry 1 and associate it with the link state of VLAN-interface 3.
[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 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 : 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 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 : Backup
Config Pri : 110 Running Pri : 110
Preempt Mode : Yes Delay Time : 5
Become Master : 2200ms left
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 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 : Backup
 Config Pri : 100 Running Pri : 100
 Preempt Mode : Yes Delay Time : 5
 Become Master : 2200ms left
 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 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 : 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 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 : Backup
 Config Pri : 100 Running Pri : 100
 Preempt Mode : Yes Delay Time : 5
 Become Master : 2200ms left
 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 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 : Backup
 Config Pri : 100 Running Pri : 100
 Preempt Mode : Yes Delay Time : 5
 Become Master : 2200ms left
 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 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 timer delay 5
 vrrp vrid 1 weight track 1 reduced 250
#
interface Vlan-interface3
 ip address 20.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/3
 port access vlan 3
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
track 1 interface vlan-interface 3
#
```
- 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 timer delay 5
```

```

vrrp vrid 1 weight track 1 reduced 250
#
interface Vlan-interface3
 ip address 30.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/3
 port access vlan 3
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
track 1 interface vlan-interface 3
#

```

- **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 timer delay 5
vrrp vrid 1 weight track 1 reduced 250
#
interface Vlan-interface3
 ip address 40.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/3
 port access vlan 3
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
track 1 interface vlan-interface 3
#

```

# IPv6-based VRRP configuration examples

This chapter provides IPv6-based VRRP configuration examples.

## Example: Configuring a single VRRP group

### Applicable product matrix

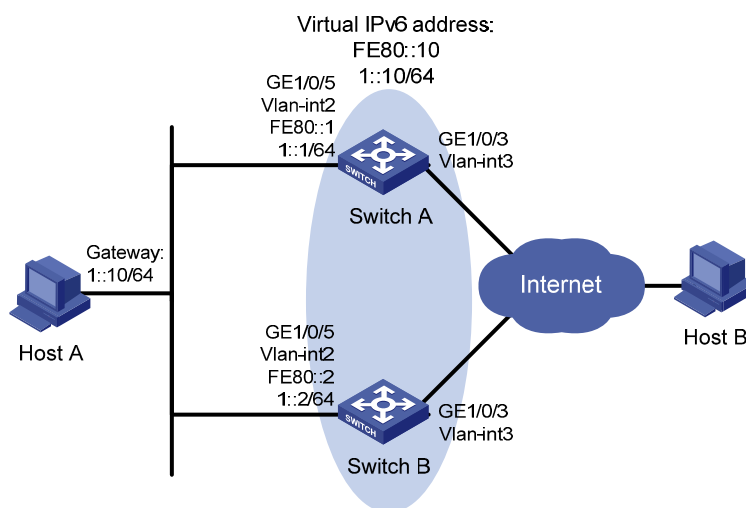
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

### 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 to forward packets from the hosts to the external network. When Switch A fails, Switch B takes over to forward packets for the hosts.
- When the uplink interface of Switch A fails, hosts can access the external network through Switch B.

**Figure 253 Network diagram**



## Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

For Host A to access the external network when the uplink interface of Switch A fails, configure VRRP tracking on Switch A. When the uplink interface of Switch A is down or removed, Switch A decreases its priority and Switch B takes over to forward packets from the hosts.

To avoid frequent role change in the VRRP group, configure a preemption delay.

To enable the switches in the VRRP group to only process authorized packets, configure VRRP authentication.

## Configuration procedures

### 1. Configure Switch A:

# Enable IPv6 globally.

```
<SwitchA> system-view
[SwitchA] ipv6
```

# Configure VLAN 3.

```
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/3
[SwitchA-vlan3] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ipv6 address 2003::2 64
[SwitchA-Vlan-interface3] quit
```

# Configure VLAN 2.

```
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
[SwitchA-Vlan-interface2] ipv6 address 1::1 64
```

# Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

# Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

# Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 authentication-mode simple hello
```

# Configure Switch A to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5 seconds to avoid frequent status switchover.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

# On VLAN-interface 2, set the interface to be tracked to VLAN-interface 3. The priority of VRRP group 1 on VLAN-interface 3 will decrement by 30 when VLAN-interface 2 fails.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 track interface vlan-interface 3 reduced 30
```

# Enable Switch A to send RA messages, so Host A can learn the default gateway address.

```
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
```

## 2. Configure Switch B:

# Enable IPv6 globally.

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

```
[SwitchB] ipv6
```

# Configure VLAN 3.

```
[SwitchB] vlan 3
```

```
[SwitchB-vlan3] port gigabitethernet 1/0/3
```

```
[SwitchB-vlan3] quit
```

```
[SwitchB] interface vlan-interface 3
```

```
[SwitchB-Vlan-interface3] ipv6 address 2004::2 64
```

```
[SwitchB-Vlan-interface3] quit
```

# Configure VLAN 2.

```
[SwitchB] vlan 2
```

```
[SwitchB-vlan2] port gigabitethernet 1/0/5
```

```
[SwitchB-vlan2] quit
```

```
[SwitchB] interface vlan-interface 2
```

```
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
```

```
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
```

# Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

# Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 authentication-mode simple hello
```

# Configure Switch B to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5 seconds to avoid frequent status switchover.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

# Enable Switch B to send RA messages, so Host A can learn the default gateway address.

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
```

## 3. Configure the hosts:

Configure the default gateway of Host A as 1::10/64. (Details not shown.)

## Verifying the configuration

# Ping Host B from Host A. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
```

```
IPv6 Standby Information:
```

```

Run Mode : Standard
Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
VRID : 1 Adver Timer : 100
Admin Status : Up State : Master
Config Pri : 110 Running Pri : 110
Preempt Mode : Yes Delay Time : 5
Auth Type : Simple Key : *****
Virtual IP : FE80::10
 1::10
Virtual MAC : 0000-5e00-0201
Master IP : FE80::1
VRRP Track Information:
Track Interface: Vlan3 State : Up Pri Reduced : 30

```

# Display detailed information about VRRP group 1 on Switch B.

```

[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Standby Information:
Run Mode : Standard
Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
VRID : 1 Adver Timer : 100
Admin Status : Up State : Backup
Config Pri : 100 Running Pri : 100
Preempt Mode : Yes Delay Time : 5
Become Master : 3600ms left
Auth Type : Simple Key : *****
Virtual IP : FE80::10
 1::10
Master IP : FE80::1

```

The output shows that Switch A is operating as the master in VRRP group 1 to forward packets from Host A to Host B.

# Ping Host B from Host A. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.

```

[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Standby Information:
Run Mode : Standard
Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
VRID : 1 Adver Timer : 100
Admin Status : Up State : Backup
Config Pri : 110 Running Pri : 80
Preempt Mode : Yes Delay Time : 5
Become Master : 3600ms left

```

```

Auth Type : Simple Key : *****
Virtual IP : FE80::10
 1::10
Master IP : FE80::2
VRRP Track Information:
Track Interface: Vlan3 State : Down Pri Reduced : 30

```

# Display detailed information about VRRP group 1 on Switch B.

```

[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Standby Information:
Run Mode : Standard
Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
VRID : 1 Adver Timer : 100
Admin Status : Up State : Master
Config Pri : 100 Running Pri : 100
Preempt Mode : Yes Delay Time : 5
Auth Type : Simple Key : *****
Virtual IP : FE80::10
 1::10
Virtual MAC : 0000-5e00-0201
Master IP : FE80::2

```

The output shows that when VLAN-interface 3 on Switch A is not available, the priority of Switch A is reduced to 80 and it becomes the backup. Switch B becomes the master to forward packets from Host A to Host B.

## Configuration files

- Switch A:

```

#
ipv6
#
vlan 2 to 3
#
interface Vlan-interface2
undo ipv6 nd ra halt
ipv6 address 1::1 64
ipv6 address FE80::1 link-local
vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
vrrp ipv6 vrid 1 virtual-ip 1::10
vrrp ipv6 vrid 1 priority 110
vrrp ipv6 vrid 1 preempt-mode timer delay 5
vrrp ipv6 vrid 1 track interface vlan-interface3 reduced 30
vrrp ipv6 vrid 1 authentication-mode simple cipher c3$bGi6EvJRLUqCKH07yY9RlrA
hcMFWhyzz
#
interface Vlan-interface3

```

```

 ipv6 address 2003::2/64
#
interface GigabitEthernet1/0/3
 port access vlan 3
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
• Switch B:
#
 ipv6
#
 vlan 2 to 3
#
interface Vlan-interface2
 undo ipv6 nd ra halt
 ipv6 address 1::2 64
 ipv6 address FE80::2 link-local
 vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 preempt-mode timer delay 5
 vrrp ipv6 vrid 1 authentication-mode simple cipher c3$IL0Gzf/m1E/Hn8eGeniH+LW
KHpeAjCyX
#
interface Vlan-interface3
 ipv6 address 2004::2/64
#
interface GigabitEthernet1/0/3
 port access vlan 3
#
interface GigabitEthernet1/0/5
 port access vlan 2
#

```

## Example: Configuring multiple VRRPv3 groups

### Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

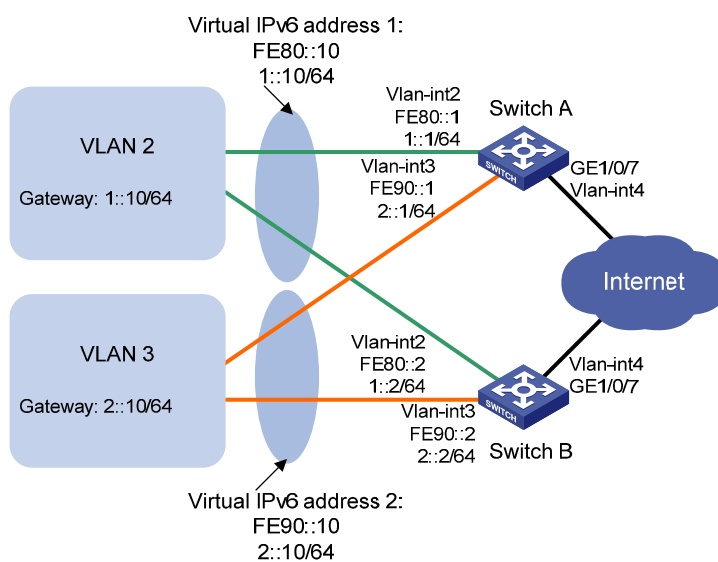


## Network requirements

As shown in [Figure 254](#), Switch A and Switch B form two VRRP groups. Implement the following requirements:

- Switch A operates as the master of VRRP group 1 to forward packets from Area A, and Switch B operates as the master of VRRP group 2 to forward packets from Area B. When one of the switches fails, the other switch provides gateway service for both areas.
- When the uplink interface of one switch fails, hosts can access the external network through the other switch.

**Figure 254 Network diagram**



## Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

For the hosts to access the external network when the uplink interface of the master in a VRRP group fails, configure VRRP tracking on the master. When the uplink interface of the master is down or removed, the master decreases its priority and the backup takes over to forward packets from the hosts.

To avoid frequent role change in the VRRP group, configure a preempt 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.

## Configuration procedures

### 1. Configure Switch A:

# Enable IPv6 globally.

```
<SwitchA> system-view
[SwitchA] ipv6
```

# Configure VLAN 4.

```
<SwitchA> system-view
[SwitchA] vlan 4
[SwitchA-vlan4] port gigabitethernet 1/0/7
[SwitchA-vlan4] quit
[SwitchA] interface vlan-interface 4
[SwitchA-Vlan-interface4] ipv6 address 2000::2 64
[SwitchA-Vlan-interface4] quit
```

# Configure VLAN 2.

```
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
[SwitchA-Vlan-interface2] ipv6 address 1::1 64
```

# Create VRRP group 1, and set its virtual IP addresses to **FE80::10** and **1::10**.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

# Assign Switch A a priority of 110 in VRRP group 1.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

# Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

# On VLAN-interface 2, configure the interface to be tracked as VLAN-interface 4. The priority of Switch A will decrement by 30 when VLAN-interface 4 is down.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 track interface vlan-interface 4 reduced 30
```

# Enable Switch A to send RA messages, so hosts in VLAN 2 can learn the default gateway address.

```
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
[SwitchA-Vlan-interface2] quit
```

# Configure VLAN 3.

```
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/6
[SwitchA-vlan3] quit
```

```
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ipv6 address fe90::1 link-local
[SwitchA-Vlan-interface3] ipv6 address 2::1 64

Create VRRP group 2, and set its virtual IP addresses to FE90::10 and 2::10.
[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip 2::10

Configure Switch A to operate in preemptive mode, and set the preemption delay to 5 seconds.
[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 preempt-mode timer delay 5

Enable Switch A to send RA messages, so hosts in VLAN 2 can learn the default gateway address.
[SwitchA-Vlan-interface3] undo ipv6 nd ra halt
```

## 2. Configure Switch B:

```
Enable IPv6 globally.
<SwitchB> system-view
[SwitchB] ipv6

Configure VLAN 4.
<SwitchB> system-view
[SwitchB] vlan 4
[SwitchB-vlan4] port gigabitethernet 1/0/7
[SwitchB-vlan4] quit
[SwitchB] interface vlan-interface 4
[SwitchB-Vlan-interface4] ipv6 address 2001::2 64
[SwitchB-Vlan-interface4] quit

Configure VLAN 2.
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
[SwitchB-Vlan-interface2] ipv6 address 1::2 64

Create VRRP group 1, and set its virtual IP addresses to FE80::10 and 1::10.
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10

Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5

Enable Switch B to send RA messages, so hosts in VLAN 2 can learn the default gateway address.
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
[SwitchB-Vlan-interface2] quit

Configure VLAN 3.
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/6
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ipv6 address fe90::2 link-local
```

```
[SwitchB-Vlan-interface3] ipv6 address 2::2 64
Create VRRP group 2, and set its virtual IP address to FE90::10 and 2::10.
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip 2::10
Assign Switch B a priority of 110 in VRRP group 2.
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 priority 110
Configure Switch B to operate in preemptive mode, and set the preemption delay to 5 seconds.
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 preempt-mode timer delay 5
On VLAN-interface 3, configure the interface to be tracked as VLAN-interface 4. The priority of
Switch B will decrement by 30 when VLAN-interface 4 is down.
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 track interface vlan-interface 4 reduced
30
Enable Switch B to send RA messages, so hosts in VLAN 2 can learn the default gateway
address.
[SwitchB-Vlan-interface3] undo ipv6 nd ra halt
```

### 3. Configure the hosts:

# Configure the default gateway of the hosts in VLAN 2 as **1::10/64** and in VLAN 3 as **2::10/64**.  
(Details not shown.)

## Verifying the configuration

# Display detailed information about the VRRP groups on Switch A.

```
[SwitchA-Vlan-interface3] display vrrp ipv6 verbose
IPv6 Standby Information:
 Run Mode : Standard
 Run Method : Virtual MAC
Total number of virtual routers : 2
Interface Vlan-interface2
 VRID : 1 Adver Timer : 100
 Admin Status : Up State : Master
 Config Pri : 110 Running Pri : 110
 Preempt Mode : Yes Delay Time : 5
 Auth Type : None
 Virtual IP : FE80::10
 1::10
 Virtual MAC : 0000-5e00-0201
 Master IP : FE80::1
VRRP Track Information:
 Track Interface: Vlan4 State : Up Pri Reduced : 30

Interface Vlan-interface3
 VRID : 2 Adver Timer : 100
 Admin Status : Up State : Backup
 Config Pri : 100 Running Pri : 100
 Preempt Mode : Yes Delay Time : 5
```

```
Become Master : 3600ms left
Auth Type : None
Virtual IP : FE90::10
 2::10
Master IP : FE90::2
```

# Display detailed information about the VRRP groups on Switch B.

```
[SwitchB-Vlan-interface3] display vrrp ipv6 verbose
```

```
IPv6 Standby Information:
```

```
Run Mode : Standard
Run Method : Virtual MAC
```

```
Total number of virtual routers : 2
```

```
Interface Vlan-interface2
```

```
VRID : 1 Adver Timer : 100
Admin Status : Up State : Backup
Config Pri : 100 Running Pri : 100
Preempt Mode : Yes Delay Time : 5
Become Master : 3600ms left
Auth Type : None
Virtual IP : FE80::10
 1::10
Master IP : FE80::1
```

```
Interface Vlan-interface3
```

```
VRID : 2 Adver Timer : 100
Admin Status : Up State : Master
Config Pri : 110 Running Pri : 110
Preempt Mode : Yes Delay Time : 5
Auth Type : None
Virtual IP : FE90::10
 2::10
Virtual MAC : 0000-5e00-0202
Master IP : FE90::2
```

```
VRRP Track Information:
```

```
Track Interface: Vlan4 State : Up Pri Reduced : 30
```

The output shows 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 Standby Information:
```

```
Run Mode : Standard
Run Method : Virtual MAC
```

```
Total number of virtual routers : 2
```

```
Interface Vlan-interface2
```

```
VRID : 1 Adver Timer : 100
Admin Status : Up State : Master
Config Pri : 100 Running Pri : 100
```

```

Preempt Mode : Yes Delay Time : 5
Auth Type : None
Virtual IP : FE80::10
 1::10
Virtual MAC : 0000-5e00-0201
Master IP : FE80::2
Interface Vlan-interface3
VRID : 2 Adver Timer : 100
Admin Status : Up State : Master
Config Pri : 110 Running Pri : 110
Preempt Mode : Yes Delay Time : 5
Auth Type : None
Virtual IP : FE90::10
 2::10
Virtual MAC : 0000-5e00-0202
Master IP : FE90::2
VRRP Track Information:
Track Interface: Vlan4 State : Up Pri Reduced : 30

```

The output shows that when Switch A fails, Switch B operates as the master in VRRP group 1 to forward Internet traffic for hosts in VLAN 2.

## Configuration files

- Switch A:

```

#
ipv6
#
vlan 2 to 4
#
interface Vlan-interface2
undo ipv6 nd ra halt
ipv6 address 1::1 64
ipv6 address FE80::1 link-local
vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
vrrp ipv6 vrid 1 virtual-ip 1::10
vrrp ipv6 vrid 1 priority 110
vrrp ipv6 vrid 1 preempt-mode timer delay 5
vrrp ipv6 vrid 1 track interface Vlan-interface4 reduced 30
#
interface Vlan-interface3
undo ipv6 nd ra halt
ipv6 address 2::1 64
ipv6 address FE90::1 link-local
vrrp ipv6 vrid 2 virtual-ip FE90::10 link-local
vrrp ipv6 vrid 2 virtual-ip 2::10
vrrp ipv6 vrid 2 preempt-mode timer delay 5
#

```

```

interface Vlan-interface4
 ipv6 address 2000::2/64
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
interface GigabitEthernet1/0/6
 port access vlan 3
#
interface GigabitEthernet1/0/7
 port access vlan 4
#

```

- Switch B:

```

#
 ipv6
#
 vlan 2 to 4
#
interface Vlan-interface2
 undo ipv6 nd ra halt
 ipv6 address 1::2 64
 ipv6 address FE80::2 link-local
 vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 preempt-mode timer delay 5
#
interface Vlan-interface3
 undo ipv6 nd ra halt
 ipv6 address 2::2 64
 ipv6 address FE90::2 link-local
 vrrp ipv6 vrid 2 virtual-ip FE90::20 link-local
 vrrp ipv6 vrid 2 virtual-ip 2::10
 vrrp ipv6 vrid 2 priority 110
 vrrp ipv6 vrid 2 preempt-mode timer delay 5
 vrrp ipv6 vrid 2 track interface Vlan-interface4 reduced 30
#
interface Vlan-interface4
 ipv6 address 2001::2/64
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
interface GigabitEthernet1/0/6
 port access vlan 3
#
interface GigabitEthernet1/0/7
 port access vlan 4
#

```

# Example: Using VRRPv3 with MSTP

## Applicable product matrix

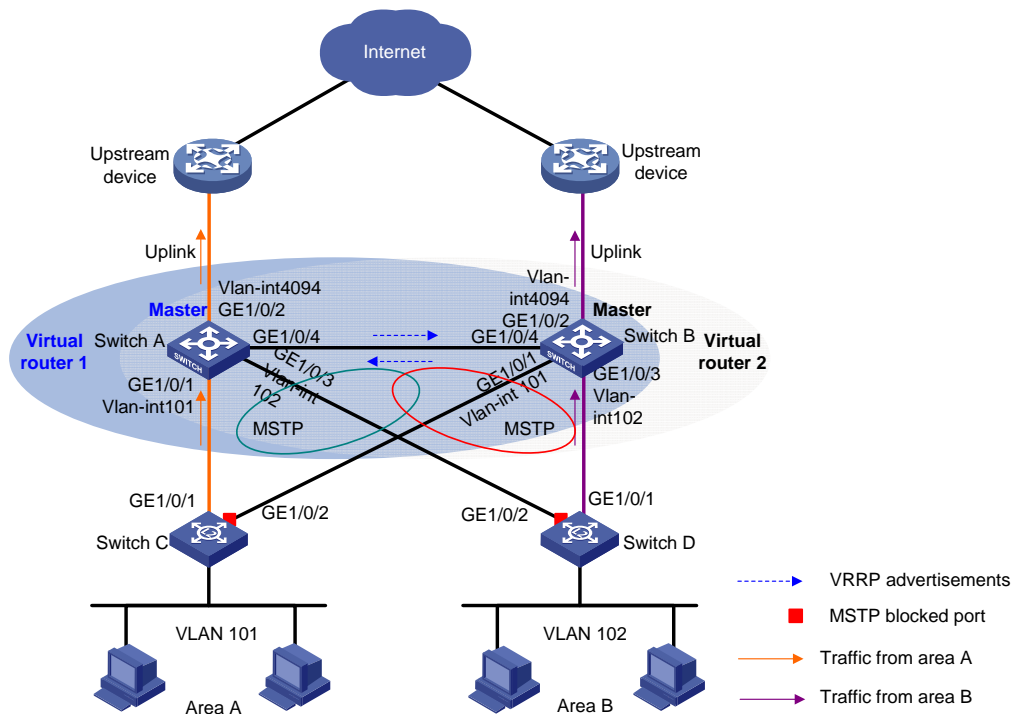
Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

## Network requirements

As shown in Figure 255, Switch A and Switch B form two VRRP groups. Implement the following requirements:

- Switch A operates as the master of VRRP group 1 to forward packets from VLAN 2, and Switch B operates as the master of VRRP group 2 to forward packets from VLAN3. When one of the switches fails, the other switch provides gateway service for both VLANs.
- When the uplink interface of one switch fails, hosts can access the external network through the other switch.

Figure 255 Network diagram





## Requirements analysis

For Switch A to become the master when it recovers, configure the preempt mode for the VRRP group.

For the hosts to access the external network when the uplink interface of the master in a VRRP group fails, configure VRRP tracking on the master. When the uplink interface of the master is down or removed, the master decreases its priority and the backup takes over to forward packets from the hosts.

To avoid loops between Switch A, Switch B, Switch C, and Switch D, enable MSTP on them.

## Configuration procedures

### 1. Configure Switch A:

# Enable IPv6 globally.

```
<SwitchA> system-view
[SwitchA] ipv6
```

# Assign GigabitEthernet 1/0/1 to VLAN 101, GigabitEthernet 1/0/3 to VLAN 102, and GigabitEthernet 1/0/2 to VLAN 4092.

```
[SwitchA] vlan 101
[SwitchA-vlan101] port gigabitethernet 1/0/1
[SwitchA-vlan101] quit
[SwitchA] vlan 102
[SwitchA-vlan102] port gigabitethernet 1/0/3
[SwitchA-vlan102] quit
[SwitchA] vlan 4092
[SwitchA-vlan4092] port gigabitethernet 1/0/2
[SwitchA-vlan4092] quit
```

# Configure the link type of GigabitEthernet 1/0/4 as trunk, and assign GigabitEthernet 1/0/4 to VLAN 101 and VLAN 102.

```
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-type trunk
[SwitchA-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[SwitchA-GigabitEthernet1/0/4] port trunk permit vlan 101 to 102
[SwitchA-GigabitEthernet1/0/4] port trunk pvid vlan 101
[SwitchA-GigabitEthernet1/0/4] quit
```

# Configure the uplink interface.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] undo stp enable
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface vlan-interface 4092
[SwitchA-Vlan-interface4092] ipv6 address 2003::2 64
```

# Create VRRP group 1.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ipv6 address fe80::2 link-local
```

```

[SwitchA-Vlan-interface101] ipv6 address 2001::2 64
[SwitchA-Vlan-interface101] vrrp ipv6 vrid 1 virtual-ip FE80::1 link-local
[SwitchA-Vlan-interface101] vrrp ipv6 vrid 1 virtual-ip 2001::1
Configure the priority of VRRP group 1 as 110.
[SwitchA-Vlan-interface101] vrrp ipv6 vrid 1 priority 110
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 interface vlan-interface 4092
reduced 20
Enable Switch A to send RA messages, so the hosts can learn the default gateway address.
[SwitchA-Vlan-interface101] undo ipv6 nd ra halt
[SwitchA-Vlan-interface101] quit
Create VRRP group 2.
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] ipv6 address fe90::2 link-local
[SwitchA-Vlan-interface102] ipv6 address 2002::2 64
[SwitchA-Vlan-interface102] vrrp ipv6 vrid 1 virtual-ip FE90::1 link-local
[SwitchA-Vlan-interface102] vrrp ipv6 vrid 1 virtual-ip 2002::1
Enable Switch A to send RA messages, so the hosts can learn the default gateway address.
[SwitchA-Vlan-interface102] undo ipv6 nd ra halt
[SwitchA-Vlan-interface102] quit
Configure MSTP.
[SwitchA] stp region-configuration
[SwitchA-mst-region] region-name vrrp
[SwitchA-mst-region] instance 1 vlan 101
[SwitchA-mst-region] instance 2 vlan 102
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
[SwitchA] stp instance 1 root primary
[SwitchA] stp instance 2 root secondary
[SwitchA] stp enable

```

## 2. Configure Switch B:

# Enable IPv6 globally.

```

<SwitchB> system-view
[SwitchB] ipv6

```

# Assign GigabitEthernet 1/0/1 to VLAN 101, GigabitEthernet 1/0/3 to VLAN 102, and GigabitEthernet 1/0/2 to VLAN 4093.

```

[SwitchB] vlan 101
[SwitchB-vlan101] port gigabitethernet 1/0/1
[SwitchB-vlan101] quit
[SwitchB] vlan 102
[SwitchB-vlan102] port gigabitethernet 1/0/3
[SwitchB-vlan102] quit
[SwitchB] vlan 4093

```

```

[SwitchB-vlan4093] port gigabitethernet 1/0/2
[SwitchB-vlan4093] quit

Configure the link type of GigabitEthernet 1/0/4 as trunk, and assign GigabitEthernet 1/0/4
to VLAN 101 and VLAN 102.

[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] port link-type trunk
[SwitchB-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[SwitchB-GigabitEthernet1/0/4] port trunk permit vlan 101 to 102
[SwitchB-GigabitEthernet1/0/4] port trunk pvid vlan 101
[SwitchB-GigabitEthernet1/0/4] quit

Configure the uplink interface.

[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] undo stp enable
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface vlan-interface 4093
[SwitchB-Vlan-interface4093] ipv6 address 2004::2 64

Create VRRP group 1.

[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ipv6 address fe80::3 link-local
[SwitchB-Vlan-interface101] ipv6 address 2001::3 64
[SwitchB-Vlan-interface101] vrrp ipv6 vrid 1 virtual-ip FE80::1 link-local
[SwitchB-Vlan-interface101] vrrp ipv6 vrid 1 virtual-ip 2001::1

Create VRRP group 2.

[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] ipv6 address fe90::3 link-local
[SwitchB-Vlan-interface102] ipv6 address 2002::3 64
[SwitchB-Vlan-interface102] vrrp ipv6 vrid 1 virtual-ip FE90::1 link-local
[SwitchB-Vlan-interface102] vrrp ipv6 vrid 1 virtual-ip 2002::1

Configure the priority of VRRP group 2 as 110.

[SwitchB-Vlan-interface102] vrrp ipv6 vrid 1 priority 110

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 interface vlan-interface 4093
reduced 20

Enable Switch B to send RA messages, so the hosts can learn the default gateway address.

[SwitchB-Vlan-interface102] undo ipv6 nd ra halt
[SwitchB-Vlan-interface102] quit

Configure MSTP.

[SwitchB] stp region-configuration
[SwitchB-mst-region] region-name vrrp
[SwitchB-mst-region] instance 1 vlan 101
[SwitchB-mst-region] instance 2 vlan 102
[SwitchB-mst-region] active region-configuration
[SwitchB-mst-region] quit
[SwitchB] stp instance 2 root primary

```

```
[SwitchB] stp instance 1 root secondary
[SwitchB] stp enable
```

### 3. Configure Switch C:

# Configure VLAN 101.

```
<SwitchC> system-view
[SwitchC] vlan 101
[SwitchC-vlan101] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[SwitchC-vlan101] quit
```

# Configure MSTP.

```
[SwitchC] stp region-configuration
[SwitchC-mst-region] region-name vrrp
[SwitchC-mst-region] instance 1 vlan 101
[SwitchC-mst-region] instance 2 vlan 102
[SwitchC-mst-region] active region-configuration
[SwitchC-mst-region] quit
[SwitchC] stp enable
```

### 4. Configure Switch D:

# Configure VLAN 102.

```
<SwitchD> system-view
[SwitchD] vlan 102
[SwitchD-vlan102] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[SwitchD-vlan102] quit
```

# Configure MSTP.

```
[SwitchD] stp region-configuration
[SwitchD-mst-region] region-name vrrp
[SwitchD-mst-region] instance 1 vlan 101
[SwitchD-mst-region] instance 2 vlan 102
[SwitchD-mst-region] active region-configuration
[SwitchD-mst-region] quit
[SwitchD] stp enable
```

### 5. Configure the hosts:

# Configure the default gateway 2001::1 for hosts in area A and 2002::1 for hosts in 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.

## Configuration files

- Switch A:  
#  
ipv6

```

#
vlan 101 to 102
#
vlan 4092
#

stp region-configuration
region-name vrrp
instance 1 vlan 101
instance 2 vlan 102
active region-configuration
#
stp instance 1 root primary
stp instance 2 root secondary
stp enable
#
interface Vlan-interface101
undo ipv6 nd ra halt
ipv6 address 2001::2/64
ipv6 address FE80::2 link-local
vrrp ipv6 vrid 1 virtual-ip FE80::1 link-local
vrrp ipv6 vrid 1 virtual-ip 2001::1
vrrp ipv6 vrid 1 priority 110
vrrp ipv6 vrid 1 track interface Vlan-interface4092 reduced 20
#
interface Vlan-interface102
undo ipv6 nd ra halt
ipv6 address 2002::2 64
ipv6 address FE90::2 link-local
vrrp ipv6 vrid 1 virtual-ip FE90::1 link-local
vrrp ipv6 vrid 1 virtual-ip 2002::1
#
interface Vlan-interface4092
ipv6 address 2003::2/64
#
interface GigabitEthernet1/0/1
port access vlan 101
#
interface GigabitEthernet1/0/2
port access vlan 4092
stp disable
#
interface GigabitEthernet1/0/3
port access vlan 102
#
interface GigabitEthernet1/0/4
port link-type trunk
undo port trunk permit vlan 1

```

```
port trunk permit vlan 101 to 102
port trunk pvid vlan 101
#
```

- Switch B:

```
#
ipv6
#
vlan 101 to 102
#
vlan 4093
#
stp region-configuration
region-name vrrp
instance 1 vlan 101
instance 2 vlan 102
active region-configuration
#
stp instance 1 root secondary
stp instance 2 root primary
stp enable
#
interface Vlan-interface101
undo ipv6 nd ra halt
ipv6 address 2001::3 64
ipv6 address FE80::3 link-local

vrrp ipv6 vrid 1 virtual-ip FE80::1 link-local
vrrp ipv6 vrid 1 virtual-ip 2001::1
#
interface Vlan-interface102
undo ipv6 nd ra halt
ipv6 address 2002::3 64
ipv6 address FE90::3 link-local
vrrp ipv6 vrid 2 virtual-ip FE90::1 link-local
vrrp ipv6 vrid 1 virtual-ip 2002::1
vrrp ipv6 vrid 2 priority 110
vrrp ipv6 vrid 1 track interface Vlan-interface4093 reduced 20
#
interface Vlan-interface4093
ipv6 address 2004::2/64
#
interface GigabitEthernet1/0/1
port access vlan 101
#
interface GigabitEthernet1/0/2
port access vlan 4093
stp disable
#
```

```
interface GigabitEthernet1/0/3
 port access vlan 102
#
interface GigabitEthernet1/0/4
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 101 to 102
 port trunk pvid vlan 101
#
```

- Switch C:

```
#
 vlan 101
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 instance 2 vlan 102
 active region-configuration
#
 stp enable
#
interface GigabitEthernet1/0/1
 port access vlan 101
#
interface GigabitEthernet1/0/2
 port access vlan 101
#
```

- Switch D:

```
#
 vlan 102
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 instance 2 vlan 102
 active region-configuration
#
 stp enable
#
interface GigabitEthernet1/0/1
 port access vlan 102
#
interface GigabitEthernet1/0/2
 port access vlan 102
#
```

# Example: Configuring VRRPv3 load balancing mode

## Applicable product matrix

Product series	Software version
HP 5500 EI	Release 2220
HP 5500 SI	

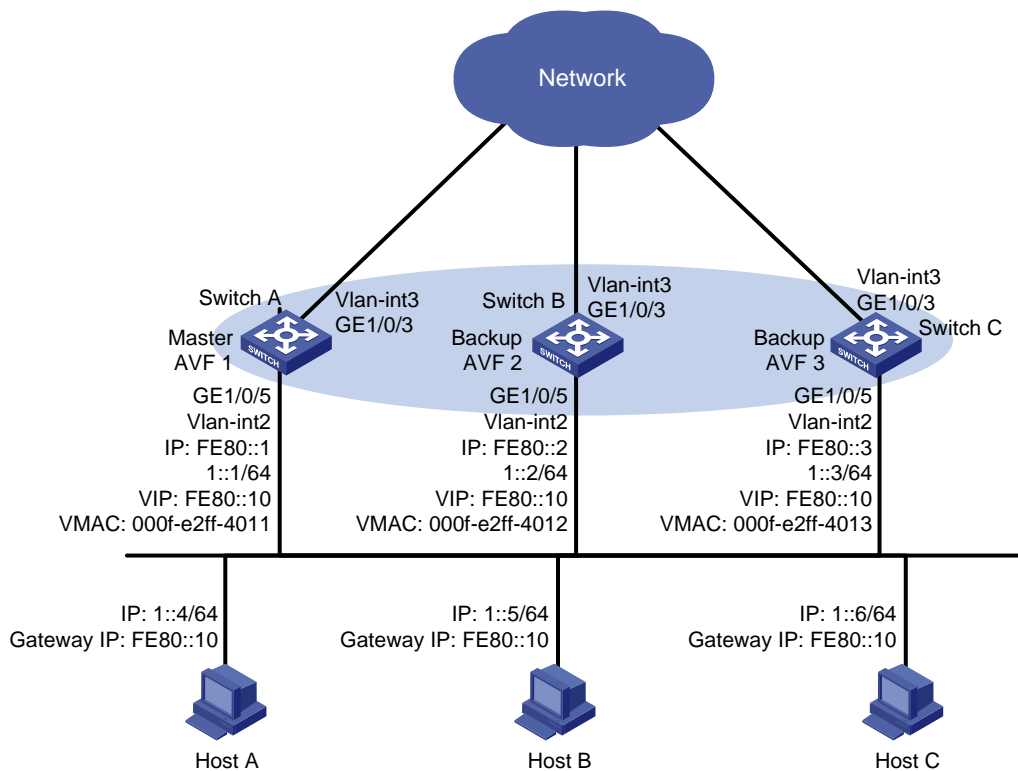
## Network requirements

As shown in [Figure 256](#), Switch A, Switch B, and Switch C form a load-balanced VRRP group to provide gateway service. Implement 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.
- When the upstream link of the active virtual forwarder (AVF) fails, the AVF can notify a listening virtual forwarder (LVF) to take over.



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.

## 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. It cannot be 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. For an LVF to become the AVF when the upstream link of the VF owner fails, the reduced weight for the VF owner must be higher than 245.
- 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.

# Enable IPv6 globally.

```
<SwitchA> system-view
[SwitchA] ipv6
```

# Configure VLAN 3.

```
<SwitchA> system-view
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/3
[SwitchA-vlan3] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ipv6 address 2003::2 64
[SwitchA-Vlan-interface3] quit
```

# Configure VLAN 2.

```
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
```

# 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 timer 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 and associate it with the link state of VLAN-interface 3.

```
[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.

# Enable IPv6 globally.

```

<SwitchB> system-view
[SwitchB] ipv6
Configure VLAN 3.
<SwitchB> system-view
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/3
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ipv6 address 2004::2 64
[SwitchB-Vlan-interface3] quit

Configure VLAN 2.
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port 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 timer 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 and associate it with the link state of VLAN-interface 3.
[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**

```

Enable IPv6 globally.
<SwitchC> system-view
[SwitchC] ipv6

Configure VLAN 3.
<SwitchC> system-view

```

```

[SwitchC] vlan 3
[SwitchC-vlan3] port 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 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 timer 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 and associate it with the link state of VLAN-interface 3.
[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 Standby Information:
 Run Mode : Load Balance
 Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
 VRID : 1 Adver Timer : 100
 Admin Status : Up State : Master

```

```

Config Pri : 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 Standby Information:
Run Mode : Load Balance
Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
VRID : 1 Adver Timer : 100
Admin Status : Up State : Backup
Config Pri : 110 Running Pri : 110
Preempt Mode : Yes Delay Time : 5
Become Master : 2200ms left
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 Standby Information:
 Run Mode : Load Balance
 Run Method : Virtual MAC
Total number of virtual routers : 1
Interface Vlan-interface2
 VRID : 1 Adver Timer : 100
 Admin Status : Up State : Backup
 Config Pri : 100 Running Pri : 100
 Preempt Mode : Yes Delay Time : 5
 Become Master : 2200ms left
 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 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 : 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 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 : Backup
 Config Pri : 100 Running Pri : 100
 Preempt Mode : Yes Delay Time : 5
 Become Master : 2200ms left
 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 after the timeout timer expired.

[SwitchC-Vlan-interface2] display vrrp ipv6 verbose

IPv6 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 : Backup  
Config Pri : 100 Running Pri : 100  
Preempt Mode : Yes Delay Time : 5  
Become Master : 2200ms left  
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 expired, 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 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 : 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 will become the master after Switch A fails.

## Configuration files

- Switch A:

```
#
ipv6
#
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 timer delay 5
 vrrp ipv6 vrid 1 weight track 1 reduced 250
#
interface Vlan-interface3
 ipv6 address 2003::2/64
#
interface GigabitEthernet1/0/3
 port access vlan 3
#
interface GigabitEthernet1/0/5
 port access vlan 2
#
track 1 interface vlan-interface 3
#

```

- Switch B:

```

#
 ipv6
#
 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 timer delay 5
 vrrp ipv6 vrid 1 weight track 1 reduced 250
#
interface Vlan-interface3
 ipv6 address 2004::2/64
#
interface GigabitEthernet1/0/3
 port access vlan 3
#
interface GigabitEthernet1/0/5

```

```

 port access vlan 2
#
track 1 interface vlan-interface 3
#
• Switch C:
#
 ipv6
#
 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 timer delay 5
 vrrp ipv6 vrid 1 weight track 1 reduced 250
#
 interface Vlan-interface3
 ipv6 address 2005::2/64
#
 interface GigabitEthernet1/0/3
 port access vlan 3
#
 interface GigabitEthernet1/0/5
 port access vlan 2
#
 track 1 interface vlan-interface 3
#

```