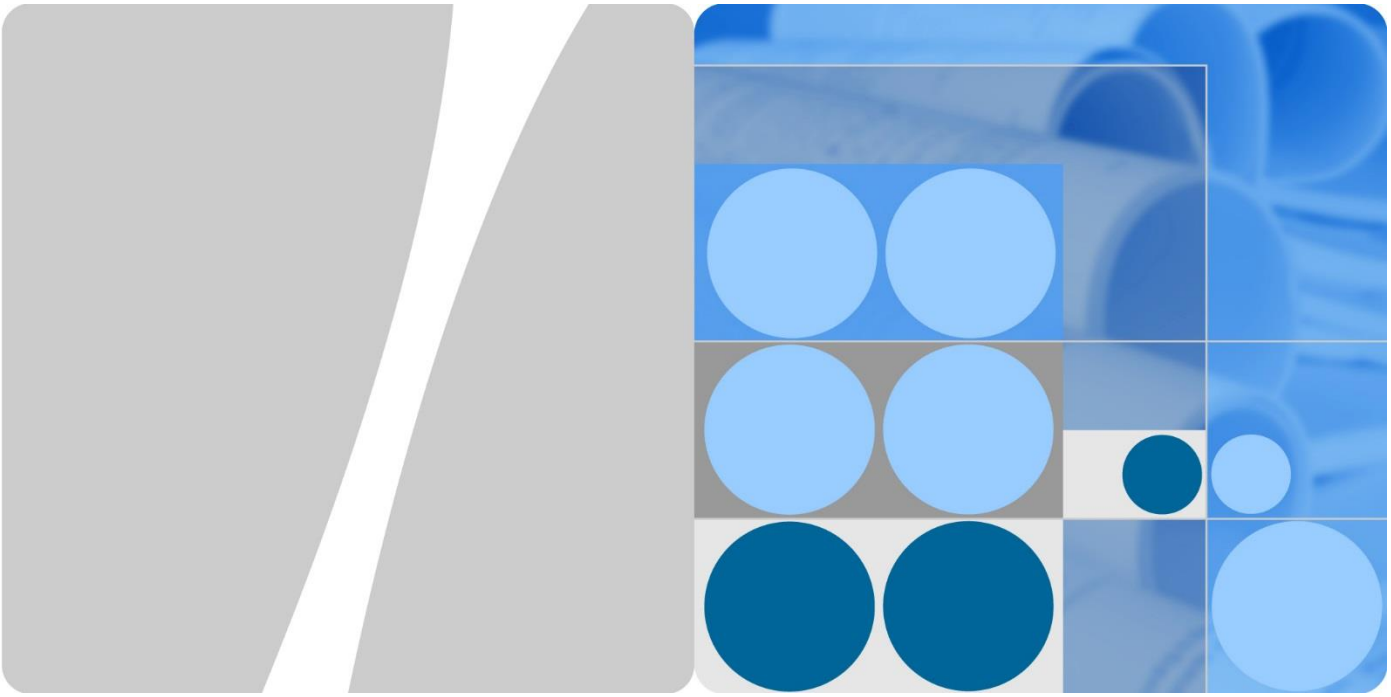


HUAWEI NE Series Routers

Configuration and Deployment Instructions

Issue 01

Date 2019-3-20

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 Configuration Instructions

About This Chapter

NOTE

This document describes the configuration instructions of NE series routers in some scenarios. When configuring and maintaining some features on NE series routers, customers must deploy services according to the configuration instructions to prevent service interruptions caused by incorrect configurations, incorrect use, or missing reliability.

1.1 Basic Configuration

1.1.1 User Login Configuration Instructions

1.1.1.1 Set the Number of SSH Server Public Keys Saved on an SSH Client to Less Than 20

When the number of SSH server public keys saved on the device reaches 20, the device can function as an SSH client to log in to a new server but does not record **ssh client x.x.x.x assign rsa-key x.x.x.x** information.

Scenario

A device functions as an SSH client, and a user uses this client to log in to an SSH server.

Configuration Requirements

The number of SSH server public keys saved on an SSH client must be smaller than 20.

Misconfiguration Risks

None

1.1.1.2 Configure ACLs for VTY Channels

If no ACL is configured for VTY channels on a device, the device is exposed to external attacks, which leads to high CPU usage.

Scenario

A user logs in to a device through Telnet or SSH.

Configuration Requirements

ACLs must be configured for VTY channels to control the calling in and calling out rights.

Misconfiguration Risks

Risk description:

If no ACL is configured for VTY channels on the device and the device is under attacks, the CPU usage becomes high, which adversely affects services.

Identification method:

Run the **display current-configuration** command in the user view to check whether the **acl** *acl-number* **inbound** | **outbound** command is configured for all VTY channels.

The command output shows that the **acl** *acl-number* **inbound** | **outbound** command is not configured for VTY channels 16 to 20.

```
<HUAWEI> display current-configuration configuration
#
user-interface vty 0 14
 acl 3100 inbound
```



```
 authentication-mode aaa
 protocol inbound ssh
user-interface vty 16 20
 authentication-mode aaa
 protocol inbound ssh
#
```

Recovery measures:

Configure ACLs for all VTY channels.

1.1.1.3 Configure ACLs for an SSH Server

If no ACL is configured for an SSH server, a large number of unauthorized users may log in to the Tacas server.

Scenario

A user logs in to the device in SSH mode, and an ACL is configured for the VTY channel.

Configuration Requirements

Run the **ssh server acl** command to filter out IP addresses of unauthorized users.

Misconfiguration Risks

Risk description:

If the **ssh server acl** command is not configured, a large number of unauthorized users may fail to log in to the Tacas server, and a large number of alarms are generated.

Identification method:

Run the **display current-configuration** command in the user view to check whether the **ssh server acl number** command is configured in the system.

```
<HUAWEI>display current-configuration configuration ssh
ssh server acl
```

Recovery measures:

Configure ACLs for an SSH server.

1.2 System Management

1.2.1 NTP Configuration Instructions

1.1.1.1 Configure the preference Parameter to Specify a Remote NTP Server to Be Preferentially Selected

When multiple remote NTP servers are specified using the **ntp-service unicast-server** *server-ip* command, the **preference** parameter must be specified for one of the servers so that this server is preferentially selected. This prevents frequent switching between different NTP servers.

Scenario

Multiple remote NTP servers are specified using the **ntp-service unicast-server** *server-ip* command in the system view.

Configuration Requirements

When multiple remote NTP servers are specified using the **ntp-service unicast-server** *server-ip* command, the **preference** parameter must be specified for one of the servers so that this server is preferentially selected.

Misconfiguration Risks

Risk description:

If multiple remote NTP servers are specified using the **ntp-service unicast-server** *server-ip* command, but the **preference** parameter is not specified for any of the servers, the NTP client frequently switches between different NTP servers, the time on the NTP client frequently changes, and a large number of logs are generated.

Identification method:

Run the **display current-configuration configuration** *ntp* command in the user view to check the configurations on the NTP client.

According to the following command output, more than one remote NTP server is configured, but the **preference** parameter is not specified for any of the servers.

```
<HUAWEI> display current-configuration configuration ntp
#
ntp-service unicast-server 10.1.1.1
ntp-service unicast-server 10.1.1.2
#
```

Recovery measures:

Run the **ntp-service unicast-server** *server-ip* **preference** command in the system view to specify a remote NTP server as the server to be preferentially selected.

1.1.1.2 Run All of the Required Commands If NTP MD5 or SHA56 Authentication Is Configured

An NTP authentication mode (MD5 or SHA56) is configured, and the **ntp-service authentication enable** command is run, but no other authentication-related commands are run. As a result, the NTP client fails to synchronize clock signals with the NTP server.

Scenario

NTP authentication is enabled on an NTP client using the **ntp-service authentication enable** command in the system view.

Configuration Requirements

The following commands must be all run in the system view to ensure that the NTP client synchronizes clock signals with the NTP server:


```
<HUAWEI> system-view
[HUAWEI] ntp-service authentication enable
[HUAWEI] ntp-service reliable authentication-keyid 169
[HUAWEI] ntp-service unicast-server 10.0.0.1 authentication-keyid 169
[HUAWEI] ntp-service authentication-keyid 169 authentication-mode md5 cipher
Root@123
```

Misconfiguration Risks

Risk description:

The NTP client fails to synchronize clock signals with the NTP server if any of the following commands is not run:

- **ntp-service authentication-keyid** *key-id* **authentication-mode** *mode* **cipher** *password*
- **ntp-service reliable authentication-keyid** *key-id key-id*
- **ntp-service unicast-server** *server-ip* **authentication-keyid** *key-id* (This command applies only to the NTP client, not to the server.)

Identification method:

Run the **display current-configuration configuration** *ntp* command in the user view to check the configurations on the NTP client.

According to the following command output, only the **ntp-service authentication enable** command is run.

```
<HUAWEI> display current-configuration configuration ntp
#
ntp-service authentication enable
#
```

Recovery measures:

Run all of the required commands in the system view.

1.2.2 NQA Configuration Instructions

1.1.1.1 Configure a Proper NQA Probe Period

The probe period configured for an NQA test instance is too short. Consequently, when a probe is still going on, the next probe begins, leading to a "no result" error. As a result, association between NQA and another protocol fails.

Scenario

An NQA test instance is configured.

Configuration Requirements

- The **stop** command must be run in the NQA view to stop the test.
- The **frequency** *interval* command must be run in the NQA view to configure an NQA probe period, with the following inequality being met:

  Frequency > (**Probe-count** – 1) x **Interval** + **Timeout**
- The **start now** command must be run in the NQA view to start the test.

Misconfiguration Risks

Risk description:

If the preceding inequality is not met, a "no result" error is reported, and other protocols, such as routing protocols and VRRP, may fail to be associated with NQA, adversely affecting service forwarding.

Identification method:

Run the **display current-configuration configuration** *nqa* command in the user view to check whether the preceding inequality is met.

According to the following command output, **frequency**, **probe-count**, **interval**, and **timeout** are 20s, 5, 6s, and 4s, respectively. The preceding inequality is not met. Therefore, a "no result" error will be reported.

```
<HUAWEI> display current-configuration configuration nqa
#
nqa test-instance 1 1
 test-type icmp
 destination-address ipv4 127.0.0.1
 frequency 20
 interval seconds 6
 timeout 4
 probe-count 5
 start now
#
```

Recovery measures:

Configure **frequency**, **probe-count**, **interval**, and **timeout** properly so that the preceding inequality is met.

1.3 Reliability

1.3.1 BFD Configuration Instructions

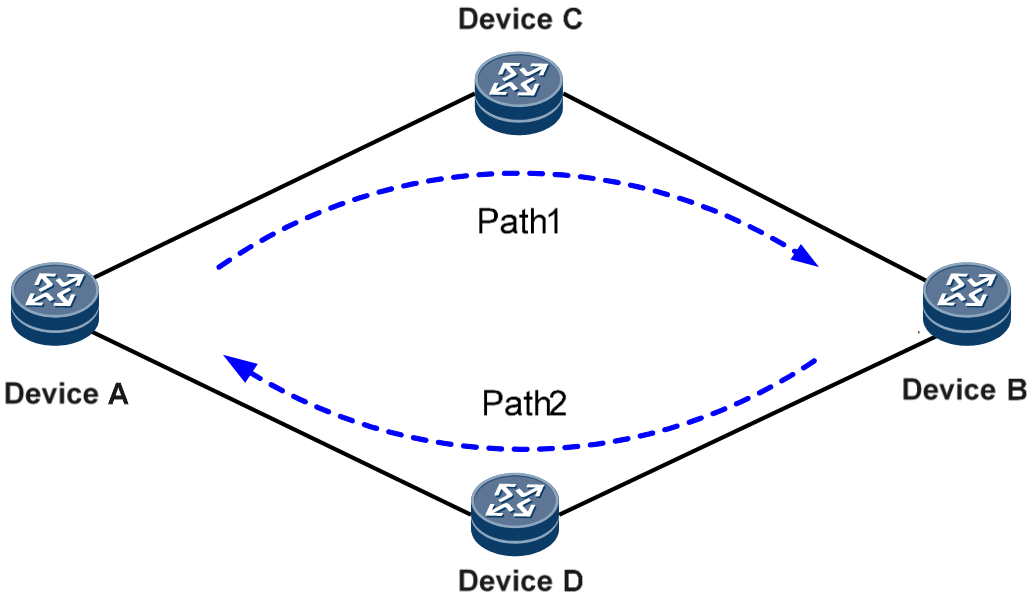
1.1.1.1 Configure Consistent Forward and Reverse Paths for a BFD for LSP Session

A BFD for LSP session is configured, and the LSP from the source device to the destination device is different from the return LSP or IP path. When the return LSP or IP path fails, the session goes down, causing an incorrect LSP switchover.

Scenario

As shown in Figure 1-1, there are two paths between Router A and Router B, path 1 and path 2.

Figure 1-1 Incorrect LSP switchovers caused by different forward and reverse paths of the BFD for LSP session



Configuration Requirements

When a BFD for LSP session is deployed on a network, the following requirements must be met:

1 For a dynamic BFD for LSP session, configure a route constraint mode to ensure that the forward and reverse paths are consistent (for example, use high-priority static routes).

2. For a static BFD for LSP session (excluding BFD for TE LSP), configure a route constraint mode to ensure that the forward and reverse paths are consistent (for example, use high-priority static routes).

3. For a static BFD for TE LSP session, configure strict explicit path constraints to ensure that the forward and reverse paths are consistent, and configure a BFD for TE LSP session on both the forward and reverse paths.

Misconfiguration Risks

Risk description:

1 A dynamic BFD for LSP session is configured, and paths 1 and 2 are the LSP and IP path, respectively.

4. A static BFD for LSP session (excluding BFD for TE LSP) is configured. The session on path 2 is configured to travel along an LSP, and the LSP is configured not to share the LSP from Router A to Router B.

5. A static BFD for TE-LSP session is configured on both paths 1 and 2, and strict explicit paths are not configured for the TE-LSPs on Router A and Router B.

When any of the preceding conditions is met, the forward and reverse paths of the BFD session are inconsistent. When the reverse path fails, the forward LSP may be incorrectly switched.

The BFD session aims to monitor path 1. However, when path 2 fails, the session goes down because the reverse path fails, triggering the LSP on path 1 to be incorrectly switched to the faulty path 2. As a result, service traffic is lost.

Identification method:

1 In this example, the forward and reverse paths of the dynamic BFD session are the LSP and IP path, respectively. The identification method depends on the network, and the forward and reverse paths of the BFD session must be consistent.

6. Check the BFD session's neighbor information on Router A.

   # Run the **display bfd session all verbose** command in the user view to check the BFD session's neighbor information from Router A to Router B. The content in bold indicates the BFD session's neighbor and next hop from Router A to Router B.

```
<HUAWEI> display bfd session all verbose
-------------------------------------------------------------------------------
-
  State : Up                Name : dyn_16396
-------------------------------------------------------------------------------
-
  Local Discriminator   : 16396          Remote Discriminator   : 16392
  Session Detect Mode   : Asynchronous Mode Without Echo Function
  BFD Bind Type         : TE_LSP
  Bind Session Type     : Dynamic
  Bind Peer IP Address  : 10.2.2.2
  NextHop Ip Address    : 10.1.1.2
  ......
```

7. Check the BFD session's neighbor information on Router B.

   # Run the **display bfd session all verbose** command in the user view to check the BFD session's neighbor information from Router B to Router A. The content in bold indicates the BFD session's neighbor from Router B to Router A.

```
<HUAWEI> display bfd session all verbose
-------------------------------------------------------------------------------
-
  (Multi Hop) State : Up                Name : dyn_16392
-------------------------------------------------------------------------------
-
  Local Discriminator   : 16392          Remote Discriminator   : 16396
  Session Detect Mode   : Asynchronous Mode Without Echo Function
  BFD Bind Type         : Peer IP Address
  Bind Session Type     : Entire_Dynamic
  Bind Peer IP Address  : 10.1.1.1
  ......
```

8. Check the routing information from Router B to Router A.

   Run the **display ip routing-table** *ip-address mask* **verbose** command in the user view to check the routing information from Router B to Router A. The content in bold indicates the BFD session's next hop from Router B to Router A. The BFD session's next hop from Router A to Router B is 10.1.1.2, but the BFD session's next hop from Router B to Router A is 10.2.1.2, indicating that the BFD session's forward and reverse paths are inconsistent.

```
<HUAWEI> display ip routing-table 10.1.1.1 32 verbose
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black
hole route
------------------------------------------------------------------------------
```



```
Routing Table : _public_
Summary Count : 1
Destination: 10.1.1.1/32
    Protocol: ISIS-L2        Process ID: 1
  Preference: 15                 Cost: 10
     NextHop: 10.2.1.2         Neighbour: 0.0.0.0
       State: Inactive Adv          Age: 1d04h15m09s
         Tag: 0                Priority: high
       Label: NULL              QoSInfo: 0x0
  IndirectID: 0xE600087A
RelayNextHop: 0.0.0.0          Interface: GigabitEthernet0/5/5
   TunnelID: 0x0                 Flags:
```

Recovery measures:

Configure consistent forward and reverse paths for a BFD for LSP session.

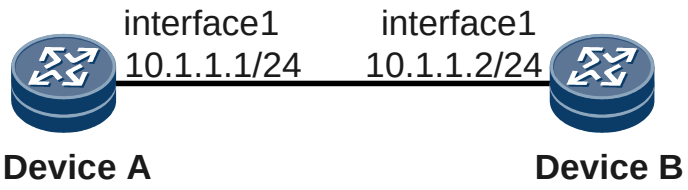
1.3.1.2 Configure Symmetric Parameters Between Both Devices of a Static BFD Session

A static BFD session is configured. When configurations on both devices are asymmetric, traffic is interrupted.

Scenario

As shown in Figure 1-2, a static BFD session is configured to detect the link between Router A and Router B.

Figure 1-2 Traffic interruption



Configuration Requirements

Symmetric local behavior parameters must be configured on both devices of a static BFD session.

- Run the **wtr** *wtr-value* command in the BFD session view on both devices to configure the same WTR time.
- Run the **process-interface-status** command in the BFD session view on both devices to associate the session with its bound interface.
- Run the **process-pst** command in the BFD session view on both devices to allow the BFD session to modify the port state table (PST).

Misconfiguration Risks

Risk description:

When any of the conditions in the configuration requirements is not met, the service switching behavior on both devices is inconsistent, causing traffic interruption.

Identification method:

1 Check the static BFD session's WTR value.

Run the **display this** command in the BFD session view on Router A. The value of **discriminator local** must match the remote discriminator on Router B. The WTR time configured on Router A is 2 minutes.

```
<HUAWEI> system-view
[HUAWEI] bfd session a
[HUAWEI-bfd-session-a] display this
#
bfd a bind peer-ip 10.1.1.2
 discriminator local 1
 discriminator remote 2
 wtr 2
 commit
#
return
```

Run the **display this** command in the BFD session view on Router B. The value of **discriminator local** must match the remote discriminator on Router A. No WTR time is configured on Router B.

```
<HUAWEI> system-view
[HUAWEI] bfd session a
[HUAWEI-bfd-session-a] display this
#
bfd a bind peer-ip 10.1.1.1
 discriminator local 2
 discriminator remote 1
 commit
#
return
```

2. Check the **process-interface-status** configuration on both devices of the static multicast BFD session.

Run the **display this** command in the BFD session view on Router A. The value of **discriminator local** must match the remote discriminator on Router B. Interface association is configured on Router A.

```
<HUAWEI> system-view
[HUAWEI] bfd session a
[HUAWEI-bfd-session-a] display this
#
bfd a bind peer-ip default-ip interface GigabitEthernet1/0/0
 discriminator local 11
 discriminator remote 12
 process-interface-status
 commit
#
return
```

Run the **display this** command in the BFD session view on Router B. The value of **discriminator local** must match the remote discriminator on Router A. Interface association is not configured on Router B.

```
<HUAWEI> system-view
```



```
[HUAWEI] bfd session a
[HUAWEI-bfd-session-a] display this
#
bfd a bind peer-ip default-ip interface GigabitEthernet1/0/0
 discriminator local 12
 discriminator remote 11
 commit
#
return
```

3. Check the **process-pst** configuration on both devices of the static BFD session.

   # Run the **display this** command in the BFD session view on Router A. The value of **discriminator local** must match the remote discriminator on Router B. PST association is configured on Router A.

```
<HUAWEI> system-view
[HUAWEI] bfd session a
[HUAWEI-bfd-session-a] display this
#
bfd a bind peer-ip 10.1.1.2 interface GigabitEthernet1/0/0
 discriminator local 11
 discriminator remote 12
 process-pst
 commit
#
return
```

   # Run the **display this** command in the BFD session view on Router B. The value of **discriminator local** must match the remote discriminator on Router A. PST association is not configured on Router B.

```
<HUAWEI> system-view
[HUAWEI] bfd session a
[HUAWEI-bfd-session-a] display this
#
bfd a bind peer-ip 10.1.1.1 interface GigabitEthernet1/0/0
 discriminator local 12
 discriminator remote 11
 commit
#
return
```

Recovery measures:

Configure symmetric parameters between both devices of a static BFD session.

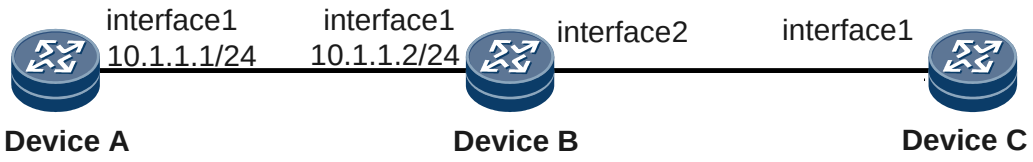
1.3.1.3 Prevent BFD Discriminator Conflicts

A static BFD session flaps because of remote discriminator conflicts.

Scenario

As shown in Figure 1-3, a static BFD session is configured to monitor the link between Router A and Router B.

Figure 1-3 Periodic BFD session flapping due to BFD discriminator conflicts



Configuration Requirements

When BFD is deployed on a network, discriminators must be uniformly planned to prevent discriminator conflicts.

Misconfiguration Risks

Risk description:

1 A static BFD session is configured on Router B, which establishes a session with Router A. The **discriminator local** *discr-value* command is run in the BFD view to set the local discriminator to **a**.

2. A static BFD session is configured on Router C, and the **discriminator remote** *discr-value* command is run in the BFD view to set the remote discriminator to **a**.

When the preceding conditions are met, the BFD session periodically flaps, causing services bound to the BFD session to flap.

The BFD session down reasons on both devices are both neighbor down.

Identification method:

1 Check the static BFD session configurations on both devices.

Run the **display this** command in the BFD session view on Router B. The value of **discriminator local** must match the remote discriminator on Router A.

```
<HUAWEI> system-view
[HUAWEI] bfd session a
[HUAWEI-bfd-session-a] display this
#
bfd a bind peer-ip 10.1.1.2
 discriminator local 1
 discriminator remote 2
 commit
#
return
```

Run the **display this** command in the BFD session view on Router A. The value of **discriminator local** must match the remote discriminator on Router B.

```
<HUAWEI> system-view
[HUAWEI] bfd session a
[HUAWEI-bfd-session-a] display this
#
bfd a bind peer-ip 10.1.1.1
 discriminator local 2
 discriminator remote 1
 commit
```



```
#
return
```

3. Check detailed information about the BFD session.

   # Run the **display bfd session all verbose** command in the user view to check detailed information about the BFD session on Router A. The BFD session enters the NeighborDown state.

```
<HUAWEI> display bfd session all verbose
--------------------------------------------------------------------------------
-
  (Multi Hop) State : Down               Name : a
--------------------------------------------------------------------------------
-
  Local Discriminator    : 1             Remote Discriminator   : 2
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Peer IP Address

  Active Multi           : -
  Last Local Diagnostic  : Neighbor Signaled Session Down
```

   # Run the **display bfd session all verbose** command in the user view to check detailed information about the BFD session on Router B. The BFD session enters the NeighborDown state.

```
<HUAWEI> display bfd session all verbose
--------------------------------------------------------------------------------
-
  (Multi Hop) State : Down               Name : a
--------------------------------------------------------------------------------
-
  Local Discriminator    : 2             Remote Discriminator   : 1
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Peer IP Address

  Active Multi           : -
  Last Local Diagnostic  : Neighbor Signaled Session Down
```

4. Check the BFD session configuration on Router C.

   # Run the **display current-configuration configuration bfd-session** command in the user view to check whether any BFD session with local discriminator conflicts exists on Router C. The value of **discriminator remote** conflicts with the remote discriminator on Router B.

```
<HUAWEI> display current-configuration configuration bfd-session
#
bfd a bind peer-ip 10.1.1.1
 discriminator local 5
 discriminator remote 1
 commit
#
return
```

Recovery measures:

Change the remote discriminator of the BFD session on Router C to a different value.

1.3.1.4 Ensure that the Forward and Reverse Paths of a Static BFD for CR-LSP Session Are Consistent

When a static BFD session is configured to detect CR-LSPs, inconsistent forward and reverse paths may cause the BFD session to go down. As a result, services may be interrupted.

Scenario

A static BFD for CR-LSP session is configured.

Configuration Requirements

When a static BFD for CR-LSP session is configured, the forward and reverse explicit paths must be consistent.

Misconfiguration Risks

Risk description:

When the forward and reverse CR-LSPs detected by the static BFD session are inconsistent, the session may go down. The detection results cannot reflect the actual CR-LSP connectivity.

The BFD session goes down, triggering a service switchover. As a result, services may be interrupted.

Identification method:

1. Run the **display current-configuration bfd-session** command in the user view to check the BFD configuration.

   As shown in the command output, the local and remote discriminators of Tunnel 0/0/27's primary LSP are 1 and 2, respectively; the local and remote discriminators of Tunnel 0/0/27's backup LSP are 3 and 4, respectively.

   ```
   <HUAWEI> display current-configuration configuration bfd-session
   #
   bfd tunnel1 bind mpls-te interface Tunnel0/0/27 te-lsp
    discriminator local 1
    discriminator remote 2
    process-pst
    commit
   #
   bfd tunnel1-back bind mpls-te interface Tunnel0/0/27 te-lsp backup
    discriminator local 3
    discriminator remote 4
    process-pst
    commit
   #
   return
   ```

2. Run the **display current-configuration interface Tunnel** command in the user view to check the TE tunnel configuration.

   As shown in the command output, the tunnel destination IP address is **192.168.1.1**, and the explicit paths of the primary and backup LSPs are **main-to-devicea** and **backup-to-devicea**, respectively.

   ```
   <HUAWEI> display current-configuration interface Tunnel 0/0/27
   #
   ```



```
interface Tunnel0/0/27
 description huawei
 mtu 1600
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 192.168.1.1
 mpls te tunnel-id 27
 mpls te record-route label
 mpls te path explicit-path main-to-devicea
 mpls te path explicit-path backup-to-devicea secondary
 mpls te backup hot-standby mode revertive wtr 60
 mpls te backup ordinary best-effort
 mpls te igp shortcut
 mpls te igp metric absolute 10
 mpls te commit
 isis enable 100
 statistic enable #
return
```

3. Run the **display mpls te tunnel-interface** *tunnel-name* command in the user view to check the tunnel's 3-tuple information.

   As shown in the command output, the session ID, ingress LSR ID, primary LSP ID, and backup LSP ID of Tunnel 0/0/27 are 27, 192.168.1.2, 3, and 32772, respectively.

```
<HUAWEI> display mpls te tunnel-interface Tunnel 0/0/27
------------------------------------------------------------------
                Tunnel0/0/27
------------------------------------------------------------------
 Tunnel State Desc   :  UP
 Active LSP         :  Primary LSP
 Session ID         :  27
 Ingress LSR ID    :  192.168.1.2    Egress LSR ID:  192.168.1.1
 Admin State        :  UP             Oper State   :  UP
 Primary LSP State     : UP
 Main LSP State      : READY             LSP ID  : 3
 Hot-Standby LSP State  : UP
 Main LSP State      : READY             LSP ID  : 32772
```

4. Check the tunnel's actual path, which is compared with the path queried on the peer device.

   Run the **display current-configuration interface tunnel 0/0/27** command to check whether **mpls te record-route** (or **mpls te record-route label**) has been configured. If **mpls te record-route** (or **mpls te record-route label**) has been configured, run the **display mpls te tunnel path lsp-id** *ingress-lsr-id session-id local-lsp-id* command to check the tunnel's actual path.

   If **mpls te record-route** (or **mpls te record-route label**) has not been configured, run the **tracert lsp te tunnel***interface-number* command.

```
<HUAWEI> display mpls te tunnel path lsp-id 192.168.1.2 27 3
 Tunnel Interface Name : Tunnel0/0/27
 Lsp ID : 192.168.1.2 :27 :3
 Hop Information
  Hop 0   192.168.1.2
  Hop 1   10.0.2.7
  Hop 2   10.0.2.8
  Hop 3   192.168.1.1
```



```
<HUAWEI> tracert lsp te Tunnel 0/0/27
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel0/0/1, press CTRL_C
to break.
  TTL   Replier          Time    Type     Downstream
  0                           Ingress   192.168.1.2/[3 ]
  1    192.168.1.1      32 ms   Egress
```

5. Run the **display explicit-path** *path-name* command in the user view to check the explicit path configuration of the tunnel.
   - If no explicit path is configured on the device or used in the tunnel configuration, configure a strict explicit path and use the path in the tunnel configuration.
   - If the configured explicit path contains less hops than the tunnel's actual path, add the missing hops to the explicit path configuration.
   - If the explicit path is configured to work in loose mode, change its working mode to strict and complete the explicit path.

```
<HUAWEI> display explicit-path main-to-devicea
1     10.231.253.26      Strict     Include
2     10.231.253.166     Strict     Include
3     10.231.253.77      Strict     Include
4     10.231.253.133     Strict     Include
5     10.231.253.53      Strict     Include
<HUAWEI> display explicit-path backup-to-devicea
1     10.231.253.162     Strict     Include
2     10.231.253.73      Strict     Include
3     10.231.253.129     Strict     Include
```

6. Check the egress of the tunnel based on the TE tunnel's destination IP address (192.168.1.1). Check information about the static BFD for CR-LSP session on the egress of the TE tunnel based on the static BFD for CR-LSP session's discriminator on the ingress.

   Run the **display bfd configuration discriminator** *local-discr-value* **verbose** command in the user view, with *local-discr-value* set to the value (**2**) of **Remote Discriminator**. Check that the corresponding TE tunnel is Tunnel 0/0/28.

```
<HUAWEI> display bfd configuration discriminator 2 verbose
------------------------------------------------------------------------------
-
  BFD Session Configuration Name : to 3
------------------------------------------------------------------------------
-
  Local Discriminator    : 2            Remote Discriminator   : 1
  BFD Bind Type         : TE_LSP
  Bind Session Type     : Static
  Bind Interface        : Tunnel0/0/28    TE LSP Type           : Primary
  TOS-EXP              : 7              Local Detect Multi     : 3
  Min Tx Interval (ms)   : 10             Min Rx Interval (ms)   : 10
  WTR Interval (ms)     : -               Process PST           : Enable
  Proc Interface Status  : Disable
  Bind Application      : LSPM | L2VPN
  Session Description    : -
------------------------------------------------------------------------------
-
```

7. Perform the preceding steps on the egress based on the obtained tunnel (for example, Tunnel 0/0/28) to find the tunnel's actual path, and compare the path with Tunnel 0/0/28's path obtained.

If the two paths are consistent except for opposite directions, no action is required. If the two paths are inconsistent, change the tunnel's actual path to the path obtained on the ingress.

Recovery measures:

Change the explicit paths to ensure that the tunnel's actual path is consistent with the path on the ingress.

1.3.1.5 Ensure that the BFD Detection Interval of the Inner-Layer Link Is Shorter than That of the Outer-Layer Link

In a multi-layer protection scenario, if the BFD detection interval of the inner-layer link is longer than that of the outer-layer link, inner-layer protection switching has not been triggered when BFD detects a fault on the outer-layer link.

Scenario

Multi-layer protection is configured. For example, BFD for RSVP, BFD for CR-LSP, or BFD for TE is configured.

Configuration Requirements

When BFD is deployed on a network and multi-layer protection is configured, the BFD detection interval of the inner-layer link must be shorter than that of the outer-layer link.

Different BFD detection intervals are configured in different scenarios. For example:

- For BFD for RSVP scenarios, see "(Optional) Adjusting BFD Parameters."
- For static BFD for CR-LSP scenarios, see "Configuring BFD Parameters on the Ingress of the Tunnel" and "Configuring BFD Parameters on the Egress of the Tunnel."
- For dynamic BFD for CR-LSP scenarios, see "(Optional) Adjusting BFD Parameters on the Ingress of the Tunnel."
- For BFD for TE scenarios, see "Configuring BFD Parameters on the Ingress of the Tunnel" and "Configuring BFD Parameters on the Egress of the Tunnel."

Misconfiguration Risks

Risk description:

In a multi-layer protection scenario, the BFD detection interval of the inner-layer link is longer than that of the outer-layer link. If the tunnel fails, the BFD session detecting the outer-layer link first detects the fault due to the shorter detection interval. The BFD session then triggers protection switching for tunnel services, which wastes inner-layer link protection switching.

In this situation, only outer-layer protection switching is used, which deteriorates overall switching performance.

A fault in the outer-layer link is detected, but the inner-layer link protection switching is not triggered. If the outer-layer link is configured with a protection path, the protection switching may degrade to outer-layer link protection, which wastes inner-layer link protection switching.

Identification method:

The following identification method applies when dynamic BFD for CR-LSP is configured to detect the inner-layer link, static BFD for TE is configured to detect the outer-layer link, and BFD for TE and BFD for CR-LSP are bound to the same tunnel interface. Identify the risk in other scenarios according to the actual situation.

Run the **display bfd session all verbose** command in the user view to check BFD detection intervals.

As shown in the command output, the detection interval of the BFD session detecting the inner-layer link (**BFD Bind Type** is **TE_LSP**) is 2664 ms, whereas the detection interval of the BFD session detecting the outer-layer link (**BFD Bind Type** is **TE_TUNNEL**) is 300 ms. That is, the BFD detection interval of the inner-layer link is longer than that of the outer-layer link.

```
<HUAWEI> display bfd session all verbose
-------------------------------------------------------------------------------
 State : Up                Name : dyn 16393
-------------------------------------------------------------------------------
 Local Discriminator   : 16393          Remote Discriminator   : 16402
 Session Detect Mode   : Asynchronous Mode Without Echo Function
 BFD Bind Type         : TE_LSP
 Bind Session Type     : Dynamic
 Bind Peer IP Address  : 10.2.2.2
 NextHop Ip Address    : 10.1.1.2
 Bind Interface        : Tunnel1        TE LSP Type          : Primary
 Tunnel ID           : 33
 FSM Board Id         : 9             TOS-EXP             : 6
 Min Tx Interval (ms)  : 999           Min Rx Interval (ms)   : 888
 Actual Tx Interval (ms): 999          Actual Rx Interval (ms): 888
 Local Detect Multi    : 48            Detect Interval (ms)   : 2664
 Echo Passive         : Disable        Acl Number           : -
 Destination Port      : 3784          TTL                 : 1
 Proc Interface Status  : Disable        Process PST          : Enable
 WTR Interval (ms)     : -             Config PST          : Enable
 Active Multi         : 3
 Last Local Diagnostic  : No Diagnostic
 Bind Application      : TE
 Session TX TmrID      : -             Session Detect TmrID   : -
 Session Init TmrID    : -             Session WTR TmrID     : -
 Session Echo Tx TmrID  : -
 Session Description   : -
-------------------------------------------------------------------------------


-------------------------------------------------------------------------------
 State : Up                Name : te
-------------------------------------------------------------------------------
 Local Discriminator   : 111           Remote Discriminator   : 111
 Session Detect Mode   : Asynchronous Mode Without Echo Function
 BFD Bind Type         : TE_TUNNEL
 Bind Session Type     : Static
 Bind Peer IP Address  : 10.2.2.2
 NextHop Ip Address    : -.-.-.-
 Bind Interface        : Tunnel1
 Tunnel ID           : 33
 FSM Board Id         : 9             TOS-EXP             : 1
 Min Tx Interval (ms)  : 100           Min Rx Interval (ms)   : 100
```



```
 Actual Tx Interval (ms): 100           Actual Rx Interval (ms): 100
 Local Detect Multi    : 3             Detect Interval (ms)   : 300
 Echo Passive         : Disable        Acl Number           : -
 Destination Port      : 3784          TTL                 : 1
 Proc Interface Status  : Disable        Process PST          : Disable
 WTR Interval (ms)     : -             Config PST           : Disable
 Active Multi         : 3
 Last Local Diagnostic  : No Diagnostic
 Bind Application      : No Application Bind
 Session TX TmrID      : -             Session Detect TmrID   : -
 Session Init TmrID    : -             Session WTR TmrID     : -
 Session Echo Tx TmrID  : -
 Session Description    : -
------------------------------------------------------------------------------

Total UP/DOWN Session Number : 2/0
```

Recovery measures:

Change the BFD detection interval of the inner-layer link to a value less than that of the outer-layer link.

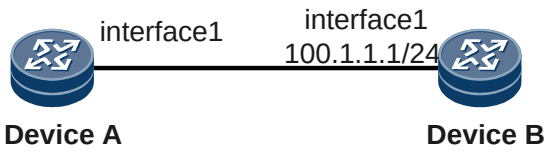
1.3.1.6 Use Symmetric BFD Configurations Between Both Devices in a Bidirectional LSP Scenario

In a bidirectional LSP scenario, when BFD configurations are asymmetric between both devices, the LDP LSP goes down. As a result, services carried on the LDP LSP are interrupted.

Scenario

As shown in Figure 1-4, LSPs exist from Router A to Router B and from Router B to Router A. BFD for peer IP is configured on Router A, and BFD for TE LSP is configured on Router B. An LDP LSP with the same peer IP address exists on Router A. If the TE LSP fails, services carried on the LDP LSP are interrupted.

Figure 1-4 Service interruption on the LDP LSP



Configuration Requirements

The same BFD type (BFD for TE LSP) must be configured on both devices.

Misconfiguration Risks

Risk description:

If the TE LSP on Router B fails, services carried on the LDP LSP are interrupted.

When the TE LSP on Router B fails, the status of the BFD session detecting the LDP LSP goes down. As a result, services carried on the LDP LSP are interrupted.

Identification method:

1 Check whether BFD configurations are symmetric between both devices.

The following information indicates that BFD configurations on both devices are asymmetric. BFD for peer IP is configured on Router A, whereas BFD for TE LSP is configured on Router B.

Run the **display current-configuration configuration bfd** command in any view on Router A.

```
<HUAWEI> display current-configuration configuration bfd
#
bfd ieclsptowac bind peer-ip 10.1.1.1
 discriminator local 101
 discriminator remote 302
 min-tx-interval 50
 min-rx-interval 50
 commit
#
```

Run the **display current-configuration configuration bfd** command in any view on Router B.

```
<HUAWEI> display current-configuration configuration bfd
#
bfd ieclsptowac bind mpls-te interface Tunnel0/0/1 te-lsp
discriminator local 302
 discriminator remote 101
 min-tx-interval 50
 min-rx-interval 50
 commit
#
```

2. Check the status of the BFD session detecting the peer IP address on Router A.

Run the **display bfd session all** command in any view of Router A. Check that the BFD session's status is down.

```
<HUAWEI> display bfd session all
--------------------------------------------------------------------------------
Local Remote    PeerIpAddr     State    Type       InterfaceName
--------------------------------------------------------------------------------
5    6        10.1.1.1      Down     S_IP_PEER       -
--------------------------------------------------------------------------------
Total UP/DOWN Session Number : 0/1
```

Run the **display mpls lsp include** *ip-address mask-len* **verbose** command in any view of Router B. Check that the status of the BFD session detecting the LDP LSP is down.

```
<HUAWEI> display mpls lsp include 10.1.1.1 32 verbose
------------------------------------------------------------------------------
             LSP Information: LDP LSP
------------------------------------------------------------------------------
  No               : 1
  VrfIndex         :
  Fec              : 10.1.1.1/32
  Nexthop          : 10.2.1.1
  In-Label         : NULL
  Out-Label        : 153468
```



```
  In-Interface       :  ----------
  Out-Interface      :  GigabitEthernet1/0/0
  LspIndex           :  191839
  Token              :  0x2001476
  FrrToken           :  0x0
  LsrType            :  Ingress
  Outgoing token     :  0x0
  Label Operation    :  PUSH
  Mpls-Mtu           :  9000
  TimeStamp          :  144908sec
  Bfd-State          :  Down
BGPKey            :  ------
```

Recovery measures:

Configure BFD for peer IP on the device where BFD for TE LSP is configured to allow BFD to go up through negotiation, and then delete the BFD configuration.

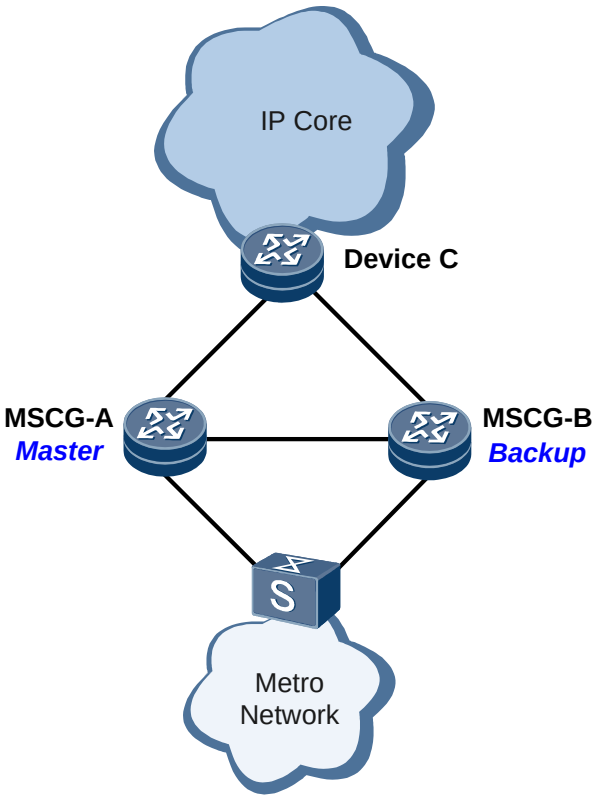
1.3.2 Multi-Device Backup Configuration Instructions

1.1.1.1 Configure a Protection Tunnel When a Shared Address Pool Is Deployed in a Dual-Device Hot Backup Scenario

A protection tunnel must be configured when a shared address pool is deployed in a dual-device hot backup scenario. If the master device's user-side link fails but no protection tunnel is configured, downstream traffic cannot enter the protection tunnel. As a result, traffic loss occurs.

Scenario

A shared address pool is deployed in dual-device hot backup scenarios, as shown in the following figure.



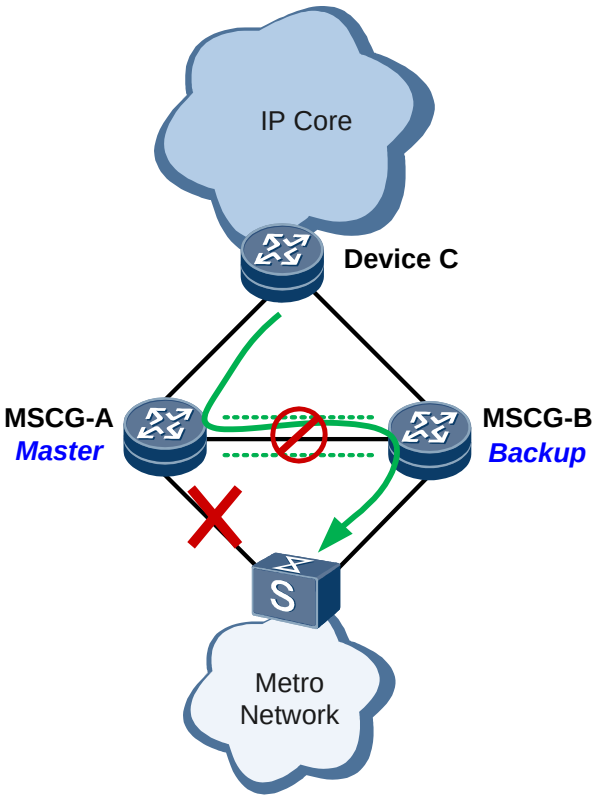
Configuration Requirements

For details, see "Configuring User Information Backup in Shared IP Address Pool Mode."

Misconfiguration Risks

Risk description:

When a shared address pool is configured in a dual-device hot backup scenario, downstream traffic arriving at the master device is switched to the backup device through a protection tunnel if the master device's user-side link fails. If no a protection tunnel is configured, downstream traffic is lost and cannot reach the user side.



Identification method:

- Run the **display remote-backup-service** *service-name* command to check all RBS information.
  - Check whether a shared address pool is bound to an RBS.

    Check whether an address pool name exists in the **ip pool** field in the command output.

    If an address pool name exists in the **ip pool** field, a shared address pool has been bound to the RBS. Go to the next step.

    If no address pool name exists in the **ip pool** field, the configuration requirements are not involved.
  - Check whether a protection tunnel is configured for the RBS.

    Check whether the command output contains the **Protect-type** and **Out-interface** fields.

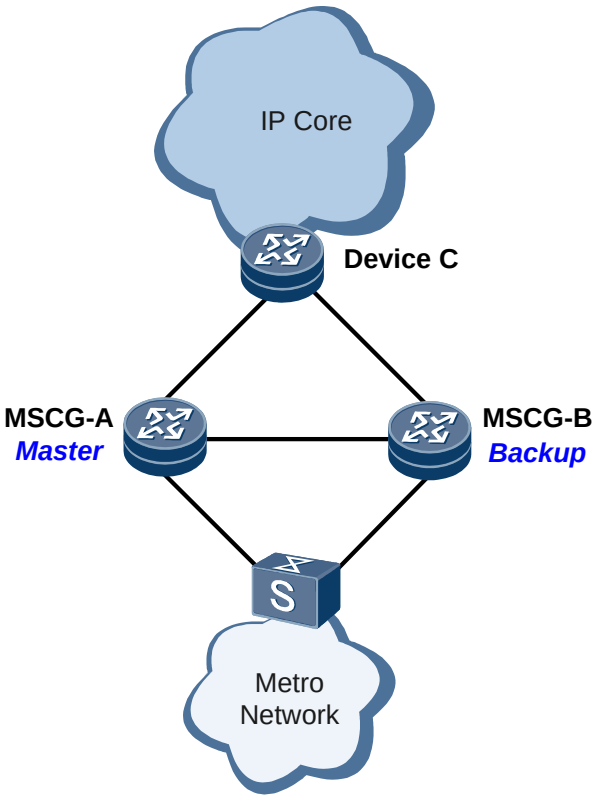
Recovery measures:

Configure a protection tunnel when a shared address pool is deployed in a dual-device hot backup scenario.

1.3.2.1 Disable URPF on a Network-Side Interface When a Shared Address Pool Is Deployed in a Dual-Device Hot Backup Scenario

Scenario

A shared address pool is deployed in dual-device hot backup scenarios, as shown in the following figure.



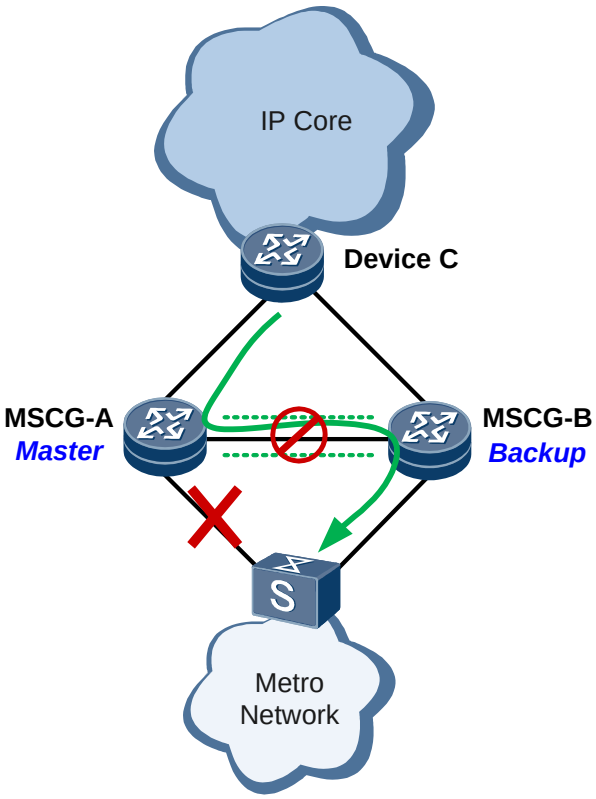
Configuration Requirements

The **undo ip urpf** command must be run on a network-side interface to disable URPF.

Misconfiguration Risks

Risk description:

When a shared address pool is configured in a dual-device hot backup scenario, traffic passes through the protection tunnel and reaches the user side if the master device's user-side link fails. If URPF is configured on the network-side interface, there is a possibility that downstream traffic cannot enter the protection tunnel. As a result, traffic loss occurs.



Identification method:

- Run the **display remote-backup-service** *service-name* command to check all RBS information.
  - Check whether a shared address pool is bound to an RBS.

    Check whether an address pool name exists in the **ip pool** field in the command output.

    If an address pool name exists in the **ip pool** field, a shared address pool has been bound to the RBS. Go to the next step.

    If no address pool name exists in the **ip pool** field, the configuration requirements are not involved.
  - Check whether a protection tunnel is configured for the RBS.

    Check whether the command output contains the **Protect-type** and **Out-interface** fields.

```
[HUAWEI] display remote-backup-service rbs
------------------------------------------------------------
 Service-Index    : 2
 Service-Name     : rbs
 TCP-State        : Initial
 Peer-ip          : 10.1.1.1
 Source-ip        : 10.6.6.3
 TCP-Port         : 6002
 Track-BFD        : --
 Uplink state     : 2 (1:DOWN 2:UP)
 Domain-map-list  : --
------------------------------------------------------------
```



```
ip pool:
      zw metric 20
ipv6 pool:
Failure ratio   : 100%
Failure duration : 0 min
-------------------------------------------------------------
Rbs-ID       : 2
Protect-type  : ip-redirect
Next-hop      : 10.1.1.2
Vlanid        : 0
Peer-ip       : 10.1.1.2
Vrfid         : 0
Tunnel-state  : UP
Tunnel-OperFlag: NORMAL
Spec-interface : GigabitEthernet1/0/2
Total users   : 0
Path 1:
   Tunnel-index  : 0x0
   Tunnel-index-v6: 0x0
   Out-interface  : GigabitEthernet1/0/2
   Vc-lable      : 4294967295
   Vc-lable-v6   : 4294967295
   User-number   : 0
   Public-Lsp-Load: FALSE

-------------------------------------------------------------
Rbs-ID       : 2
Protect-type  : public(LSP)
Peer-ip       : 10.17.17.17
Vrfid         : 4091
Tunnel-state  : UP
Tunnel-OperFlag: NORMAL
Spec-interface : Null
Total users   : 0
Path 1:
   Tunnel-index  : 0x400000f
   Tunnel-index-v6: 0x0
   Out-interface  : GigabitEthernet2/0/1
   Vc-lable      : 4294967295
   Vc-lable-v6   : 4294967295
   User-number   : 0
   Public-Lsp-Load: TRUE
```

- Run the **display this** command in the network-side interface view to check whether URPF is configured.

```
[HUAWEI -GigabitEthernet2/0/1] display this
#
interface GigabitEthernet2/0/1
 description ith
 undo shutdown
 ipv6 enable
 ip address 10.0.0.17 255.255.255.0
 ipv6 address 13:16::2/64
 mpls
```



```
mpls ldp
undo dcn
ip urpf strict
ipv6 urpf strict
#
```

Recovery measures:

Disable URPF on a network-side interface when a shared address pool is deployed in a dual-device hot backup scenario.

1.3.3 VRRP Configuration Instructions

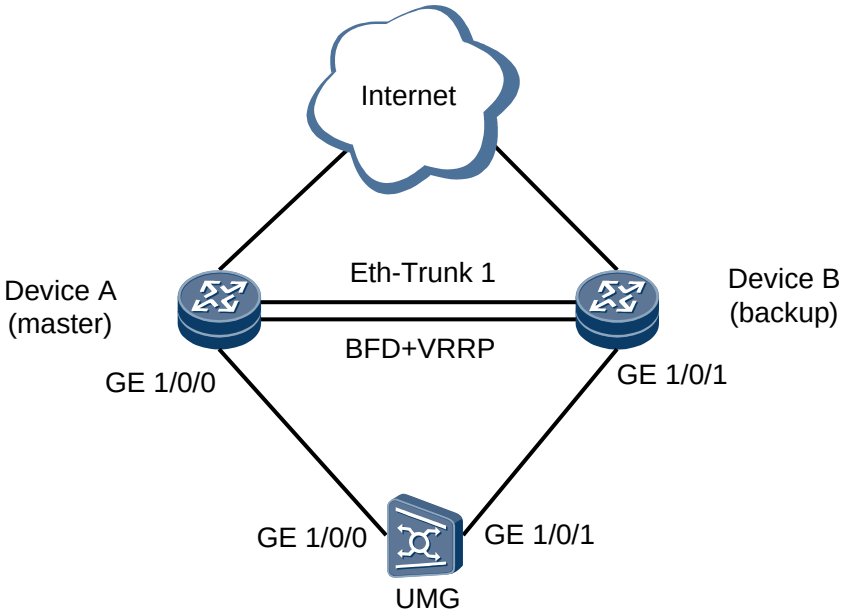
1.1.1.1 Configure Eth-Trunk Protection for the Link Between VRRP Devices

In a VRRP scenario, if inter-interface backup (only one interface forwards traffic in normal cases) is used for the upstream gateway of access devices and the interface that forwards traffic fails, the backup interface starts to forward traffic. If heartbeat packets are lost between VRRP devices, two master VRRP devices appear. As a result, traffic on the access devices may be interrupted.

Scenario

On the network shown in Figure 1-5, inter-interface backup is used for the UMG's GE 1/0/0 and GE 1/0/1. Only one interface is enabled to forward traffic. VRRP is deployed on Device A and Device B, and Eth-Trunk protection is configured for the link between the devices.

Figure 1-5 Eth-Trunk protection for the link between the VRRP devices



Configuration Requirements

A VRRP backup group must be configured on Device A and Device B. A high priority is set for Device A so that Device A functions as the master device. A low priority is set for Device B so that Device B functions as the backup device.

An Eth-Trunk interface must be configured on both Device A and Device B. Ethernet physical interfaces on different boards are added to the Eth-Trunk interface to ensure that the Eth-Trunk still has an up link after a board fails.

Misconfiguration Risks

Risk description:

There is a high probability that services on the UMG are interrupted if the heartbeat link of the Eth-Trunk interface's member interface fails and the following conditions are met:

- The UMG's interfaces support only inter-interface backup. That is, only one interface is up.
- The interfaces of the heartbeat link between Device A and Device B do not use the inter-board trunk mode.

Identification method:

NOTE
The **display interface eth-trunk** command must be run on both Device A and Device B to check whether inter-board member interfaces exist.

1 Check whether the Eth-Trunk interface's member interfaces are inter-board member interfaces.

```
<HUAWEI> display interface eth-trunk 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Link quality grade : GOOD
Description:HUAWEI, Eth-Trunk1 Interface
Switch Port, TPID : 8100(Hex), Hash arithmetic : According to flow,Maximal BW:
2G, Current BW: 1G, The Maximum Transmit Unit is 1500
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-82d9-e71b
Physical is ETH TRUNK
Current system time: 2017-04-11 12:15:41
   Last 300 seconds input rate 0 bits/sec, 0 packets/sec
   Last 300 seconds output rate 0 bits/sec, 0 packets/sec
   Realtime 2 seconds input rate 0 bits/sec, 0 packets/sec
   Realtime 2 seconds output rate 0 bits/sec, 0 packets/sec
   Input: 3 packets,939 bytes
         0 unicast,0 broadcast,3 multicast
         0 errors,0 drops
   Output:3 packets,917 bytes
         0 unicast,0 broadcast,3 multicast
         0 errors,0 drops
   Input bandwidth utilization  :    0%
   Output bandwidth utilization :    0%
-------------------------------------------------
PortName                  Status     Weight
-------------------------------------------------
GigabitEthernet1/1/8        DOWN       1
GigabitEthernet3/1/0        UP         1
```



```
-------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 1
```

2. If the Eth-Trunk interface has multiple member interfaces and the member interfaces are located on different boards (for example, GigabitEthernet 1/1/8 and GigabitEthernet 3/1/0 are located on the boards in slots 1 and 3, respectively), the risk does not exist. If the member interfaces are located on the same board, the risk exists.

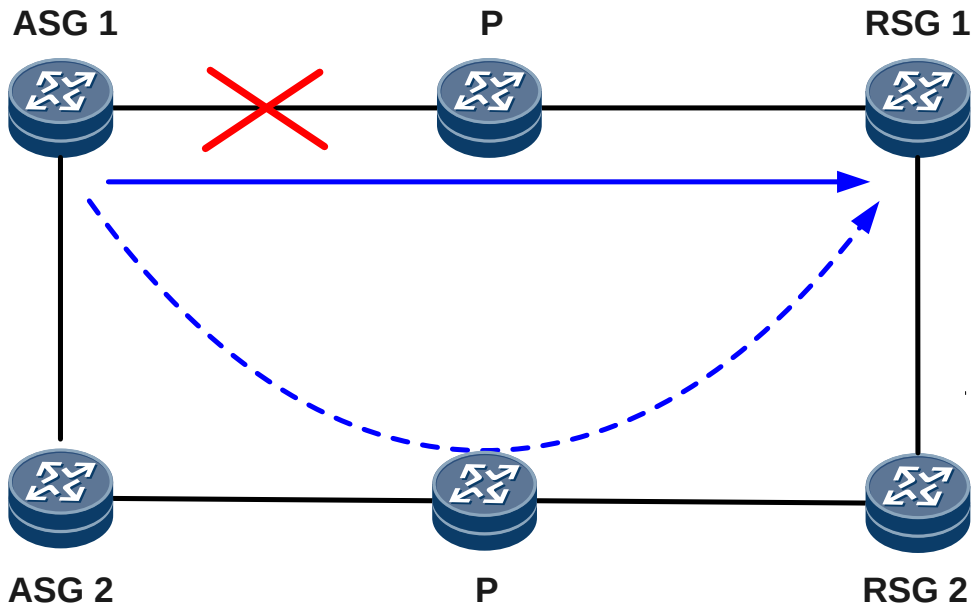
Recovery measures:

Configure an Eth-Trunk interface on both Device A and Device B. Add Ethernet physical interfaces on different boards to the Eth-Trunk interface to ensure that the Eth-Trunk still has an up link after a board fails.

1.3.4 Configure Bit-Error-triggered Protection Switching for a TE Tunnel

Scenario

As shown in the following figure, TE hot standby is deployed on an ASG and RSG in the IP RAN scenario.



Configuration Requirements

The **mpls te bit-error-detection** command must be run on the ASG's tunnel interface to configure bit-error-triggered RSVP-TE tunnel switching.

Misconfiguration Risks

Risk description:

If bit-error-triggered protection switching has not been configured and bit errors occur on the transmission device between the ASG and RSG, services on the base station connected to the ASG are interrupted.

Identification method:

Check whether bit-error-triggered protection switching has been configured on the ASG's tunnel interface.

Recovery measures:

Configure bit-error-triggered protection switching for a TE tunnel.

1.4 Interface Management

1.4.1 Interface Management Configuration Instructions

1.1.1.1 Configure a Signal Sending Delay for a Physical Interface

Scenario

1. Scenario 1: When a Huawei device is dual-homed to non-Huawei devices, the Huawei device cannot control traffic switching on the non-Huawei device interfaces.
2. Scenario 2: When a Huawei device is directly connected to a non-Huawei device, the Huawei device is powered off and then restarted, but the device does not complete configuration restoration.

Configuration Requirements

A signal sending delay must be configured for an interface using the **port-tx-enabling-delay** *port-tx-delay-time* command. After the interface is initialized, the interface does not send signals until the configured delay expires. This prevents data loss caused by synchronous link switching failure or configuration restoration failure. For details about the configuration, see "Enabling the Signal Sending Delay Function" in the product manual.

NOTE

You need to consider services that have been configured on the device when configuring a signal sending delay.

Misconfiguration Risks

Risk description:

In scenario 1, the Huawei device and non-Huawei devices may not synchronously complete link switching. If the Huawei device interface sends signals immediately after being initialized, some data may be lost.

In scenario 2, if the Huawei device interface sends signals immediately after being initialized, some data may be lost.

Identification method:

Run the **display port-tx-enabling-delay** command in the user view to check the delay configuration and delay status. The following uses the command output on a GE interface as an example. If **setted port-tx-enabling delay time is** is 0, the risk exists.


```
<HUAWEI> display port-tx-enabling-delay interface gigabitethernet 1/0/0
GigabitEthernet 1/0/0 setted port-tx-enabling delay time is: 100 ms
GigabitEthernet 1/0/0 remanent time of enabling port-tx is: 20 ms
```

Recovery measures:

Configure a signal sending delay for an interface using the **port-tx-enabling-delay** *port-tx-delay-time* command.

1.4.1.2 Configure a Hold-off Time to Respond to an Interface Down Event or Report an Interface Down Alarm

Scenario

A Huawei device connects to a WDM or transmission device through physical interfaces.

Configuration Requirements

- **Ethernet/GE/10G LAN/40GE/100GE**

  A hold-off time for a device to respond to an interface down event must be set using the **carrier down-hold-time** *interval* command. For details about the configuration, see "Configuring the Hold-Time Interval After an Interface Goes up/Down" in the product manual.

- **Other interfaces**

  A hold-off time must be set for the device management module to report an interface down alarm using the **transmission-alarm holdoff-timer** *holdoff-time* command. For details about the configuration, see "Configuring a Transmission Alarm Filtering Interval" in the product manual.

Misconfiguration Risks

Risk description:

Switching of the WDM or transmission device causes the Huawei device interface to flap frequently, resulting in a service interruption on the device interface.

Identification method:

Run the **display current-configuration** [**interface** [*interface-type* [*interface-number*]]] command in the user view to check the hold-off time for the device to respond to an interface down event. The following uses the command output on a GE interface as an example. If **carrier down-hold-time** is 0, the risk exists.

```
<HUAWEI> display current-configuration interface GigabitEthernet 1/0/0
interface GigabitEthernet1/0/0
carrier down-hold-time 100
carrier up-hold-time 10
```

Run the **display transmission-alarm configuration** [*wan interface-number* | *pos interface-number* | *e1 interface-number* | *cpos interface-number* | *wdm interface-number*] command in the user view to check alarm customization and suppression configurations on a specified interface. The following uses the command output on a GE (WAN) interface as an example. If **Holdtime** is 0, the risk exists.

```
<HUAWEI> display transmission-alarm  configuration  wan 7/1/5
```



```
2018-02-07 18:11:40.328 +08:00
 Interface: wan7/1/5
  Filter function: enabled (Holdtime is 100)
  Damping function: disable
```

Recovery measures:

For an Ethernet/GE/10G LAN/40GE/100GE interface, configure a hold-off time for a device to respond to an interface down event using the **carrier down-hold-time** *interval* command. For other interfaces, configure a hold-off time for the device management module to report an interface down alarm using the **transmission-alarm holdoff-timer** *holdoff-time* command.

1.5 LAN Access and MAN Access

1.5.1 MAC Configuration Instructions

1.1.1.1 Configure the Aging Time of MAC Address Entries to Be Longer Than or Equal to the ARP Entry Aging Time When the Upstream Traffic Is Light on a Layer 2 Device

When the upstream traffic is light on a Layer 2 device, the aging time of MAC address entries must be longer than or equal to the ARP entry aging time.

Scenario

NOTE

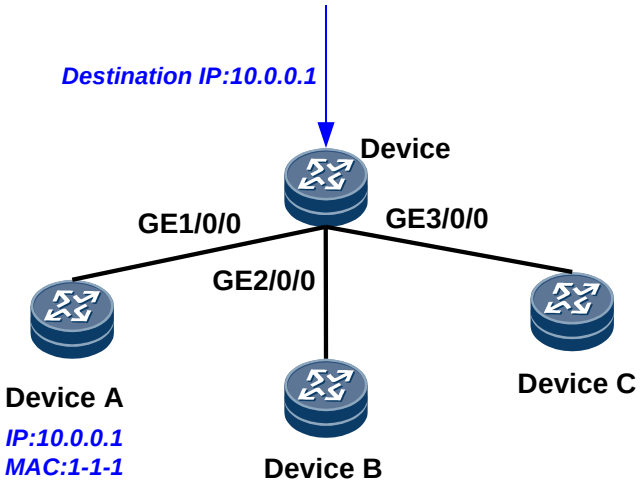
Only the LPUF-50/LPUI-21-L/LPUF-50-L/LPUF-51/LPUI-51/LPUS-51/LPUF-101/LPUI-101/LPUS-101/LPUI-51-E/LPUF-51-E/LPUF-102/LPUF-102-E/LPUI-102-E/LPUF-120/LPUF-120-E/LPUI-120/LPUS-120/LPUF-240/LPUF-240-E/LPUI-240/LPUI-52-E/LPUI-120-E/LPUF-200-E boards are involved in this scenario.

In the following figure, Device is connected to three Layer 2 devices Device A, Device B, and Device C through GE 1/0/0, GE 2/0/0, and GE 3/0/0, respectively. The three interfaces are added to VLAN 10 with interface VLANIF10 configured. GE 1/0/0 learns Device A's ARP entry and MAC address. When the downstream traffic destined for IP address 10.0.0.1 arrives at Device, Device looks up its routing table based on the destination IP address and then searches for the ARP entry based on the obtained next hop IP address. According to the ARP entry, Device obtains the VLAN ID and MAC address and then looks up the MAC address table for the outbound interface. After obtaining the outbound interface in the MAC address table, Device forwards traffic to GE 1/0/0 (the outbound interface), which then forwards traffic to Device A.

In the preceding scenario, the ARP entry and MAC address entry on Device can be updated in either of the following ways:

- Device automatically checks the entries at a specified interval according to the set aging time.
- Device updates the entries according to the upstream traffic from the Layer 2 device.

If Device A sends only little traffic to Device, Device updates the ARP and MAC address entries only through periodic ARP check.



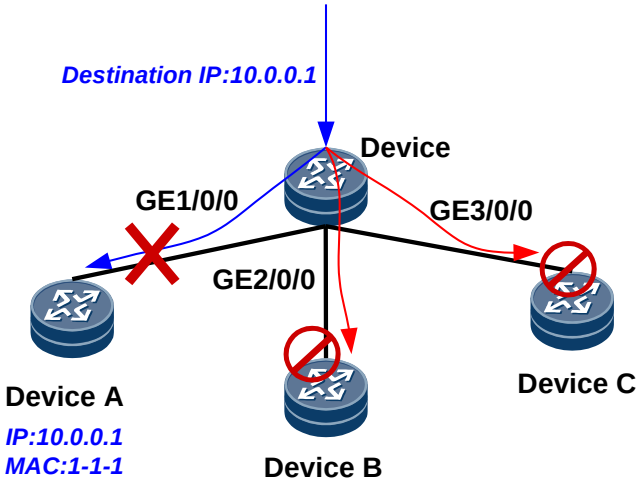
Configuration Requirements

1. The ARP entry aging time must be first queried using the **display this** command run in the interface view. If there is no **arp expire-time** in the command output, the ARP entry aging time is 1200 seconds (default value). If there is **arp expire-time** in the command output, the ARP entry aging time is **arp expire-time**.
2. The aging time of the MAC address entry must be longer than or equal to the preceding ARP entry aging time. The aging time of the MAC address entry is set using the **mac-address aging-time** *seconds* command run in the system view. The default aging time for MAC address entries is 300 seconds.

Misconfiguration Risks

Risk description:

If Device A sends only little traffic to Device, Device updates the ARP and MAC address entries only through periodic ARP check. If the aging time of the MAC address entry is shorter than that of the ARP entry on Device, Device A's MAC address entry is aged before its ARP entry. When Device receives traffic destined for Device A, it cannot find Device A's MAC address entry and therefore broadcasts traffic in VLAN 10. Both Device B and Device C receive the traffic that is not destined for them, affecting their normal services.



Identification method:

1. Run the **display this** command in the interface view to check the ARP entry aging time. If there is no **arp expire-time** in the command output, the ARP entry aging time is 1200 seconds (default value). If there is **arp expire-time** in the command output, the ARP entry aging time is **arp expire-time**.

   For example, in the following command output, there is no **arp expire-time**. The ARP aging time is therefore 1200 seconds.

   ```
   [HUAWEI-GigabitEthernet1/0/0] display this
   #
   interface GigabitEthernet1/0/0
    portswitch
    undo shutdown
    port link-type access
    port default vlan 10
   #
   return
   ```

2. Run the **display mac-address aging-time** command in the system view to check the aging time of the MAC address entry. If the aging time is shorter than the preceding ARP entry aging time, the risk exists. For example, in the following command output, the aging time of the MAC address entry is 300 seconds, indicating that the risk exists.

   ```
   <HUAWEI> display mac-address aging-time
     Aging time: 300 second(s)
   ```

Recovery measures:

Configure the aging time of MAC address entries to be longer than or equal to the ARP entry aging time.

1.5.2 Eth-Trunk Configuration Instructions

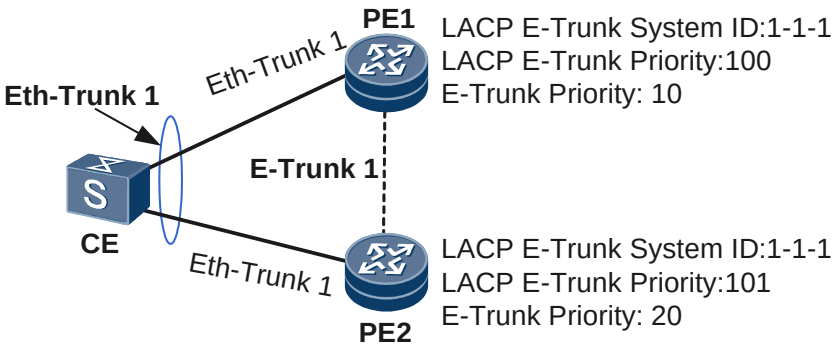
1.1.1.1 Configure Consistent Global Configurations Between Two E-Trunk Devices

In a scenario where Eth-Trunk interfaces in static LACP mode are added to an E-Trunk on two devices, the global configurations of **lacp e-trunk system-id** *system-id* and **lacp e-trunk priority** *priority* must be consistent between the two devices. Inconsistent configurations cause the Eth-Trunk interface status to be inconsistent with the expected status.

Scenario

On the network shown in Figure 1-6, Eth-Trunk 1 is configured to work in static LACP mode and added to an E-Trunk.

Figure 1-6 Inconsistent global LACP E-Trunk configurations



For details about how to configure an Eth-Trunk interface to work in static LACP mode, see Eth-Trunk interface features that the NE40E&NE80E supports.

Configuration Requirements

After Eth-Trunk interfaces are configured to work in static LACP mode and added to an E-Trunk deployed on PE1 and PE2, the **lacp e-trunk system-id** *system-id* and **lacp e-trunk priority** *priority* commands must be run on PE1 and PE2 in their system views, with system IDs being the same and priorities being the same.

Misconfiguration Risks

Risk description:

If the E-Trunk system IDs and priorities of PE1 and PE2 are not the same, the Eth-Trunk status may be inconsistent with the expected master/backup status.

Identification method:

Run the **display eth-trunk** *eth-trunk-id* command in any view of PE1 and PE2 to check **System ID** and **System Priority**. If PE1 and PE2 do not have the same system ID and system priority configurations, the risk exists.

The following command output shows that PE1 and PE2 have the same system ID but different priorities.

On PE1, Eth-Trunk 1 is added to E-Trunk 1, **System Priority** is 100, and **System ID** is 0001-0001-0001.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] display this
#
interface Eth-Trunk1
 mode lacp-static
 e-trunk 1
#
[HUAWEI] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                WorkingMode: STATIC
Preempt Delay: Disabled    Hash arithmetic: According to flow
```



```
System Priority: 100      System ID: 0001-0001-0001
Least Active-linknumber: 1  Max Active-linknumber: 16
Operate status: down      Number Of Up Port In Trunk: 0
--------------------------------------------------------------------------------
ActorPortName        Status   PortType PortPri PortNo PortKey PortState Weight
Partner:
--------------------------------------------------------------------------------
ActorPortName        SysPri   SystemID      PortPri PortNo PortKey PortState
```

On PE2, Eth-Trunk 1 is added to E-Trunk 1, **System Priority** is 101, and **System ID** is 0001-0001-0001.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] display this
#
interface Eth-Trunk1
 mode lacp-static
 e-trunk 1
#
[HUAWEI] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1               WorkingMode: STATIC
Preempt Delay: Disabled    Hash arithmetic: According to flow
System Priority: 101      System ID: 0001-0001-0001
Least Active-linknumber: 1  Max Active-linknumber: 16
Operate status: up      Number Of Up Port In Trunk: 0
--------------------------------------------------------------------------------
ActorPortName        Status   PortType PortPri PortNo PortKey PortState Weight
Partner:
--------------------------------------------------------------------------------
ActorPortName        SysPri   SystemID      PortPri PortNo PortKey PortState
```

Recovery measures:

Run the **lacp e-trunk system-id** *system-id* and **lacp e-trunk priority** *priority* commands on PE1 and PE2 to modify their system IDs to be the same and priorities to be the same.

1.5.2.2 Configure Eth-Trunk Interfaces to Work in Static LACP Mode or Bind Eth-Trunk Member Interfaces to BFD Sessions

To allow immediate detection of link faults, Eth-Trunk interfaces must work in static LACP mode, or Eth-Trunk member interfaces must be bound to BFD sessions.

Scenario

Eth-Trunk interfaces are configured on devices.

Configuration Requirements

Eth-Trunk interfaces must be configured to work in static LACP mode, or Eth-Trunk member interfaces must be bound to BFD sessions.

- When an Eth-Trunk interface works in static LACP mode, setting the LACP timeout period to the default value of 3s is recommended.

- When Eth-Trunk member interfaces need to be bound to BFD sessions, configuring a BFD WTR time is recommended.

Misconfiguration Risks

Risk description:

If an Eth-Trunk interface does not work in static LACP mode and its member interfaces are not bound to BFD sessions, Eth-Trunk member link failures cannot be detected in real time, and services cannot be switched immediately. When Eth-Trunk member interfaces are bound to BFD sessions but delayed BFD switchback (WTR time) is not configured, BFD sessions frequently flap, causing the Eth-Trunk member interfaces to frequently flap and affecting service convergence.

Identification method:

1. Check whether Eth-Trunk interfaces are configured to work in static LACP mode.

   The following command output shows that Eth-Trunk 1 is configured to work in static LACP mode but Eth-Trunk 2 and Eth-Trunk 3 are not configured to work in static LACP mode. Eth-Trunk 2 and Eth-Trunk 3 may experience the described problem. Go to the next step to continue the check.

```
<HUAWEI> display current-configuration interface Eth-Trunk
……
#
interface Eth-Trunk1
mode lacp-static
#
interface Eth-Trunk2
#
interface Eth-Trunk3
#
```

2. Check whether all the Eth-Trunk member interfaces are bound to BFD sessions.

   The following command output shows that Eth-Trunk 2's member interface GigabitEthernet1/0/0 is bound to a BFD session but member interface GigabitEthernet3/0/0 is not bound to any BFD session. Eth-Trunk 3's two member interfaces are bound to BFD sessions but do not have the WTR time configured.

   Therefore, both Eth-Trunk 2 and Eth-Trunk 3 have the problem described in this topic.

   # Check Eth-Trunk member interfaces.

```
<HUAWEI> display eth-trunk 2
Eth-Trunk2's state information is:
WorkingMode: NORMAL       Hash arithmetic: According to flow
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber:
16
Operate status: up        Number Of Up Port In Trunk: 2
--------------------------------------------------------------------
------------------
PortName                  Status     Weight
GigabitEthernet1/0/0           Up         1
GigabitEthernet3/0/0           Up         1
<HUAWEI> display eth-trunk 3
Eth-Trunk3's state information is:
WorkingMode: NORMAL       Hash arithmetic: According to flow
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber:
```



```
16
Operate status: up        Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
PortName                  Status     Weight
GigabitEthernet2/0/0           Up         1
GigabitEthernet4/0/0           Up         1
```

Check whether all the Eth-Trunk member interfaces are bound to BFD sessions.

```
<HUAWEI> display current-configuration configuration bfd-session
#
bfd eth-trunk2-1 bind peer-ip default-ip interface GigabitEthernet1/0/0
 discriminator local 6013
 discriminator remote 6213
 wtr 10
 process-interface-status
 commit
//Member interface GigabitEthernet3/0/0 is not bound to any BFD session.
#
bfd eth-trunk3-1 bind peer-ip default-ip interface GigabitEthernet2/0/0
 discriminator local 6013
 discriminator remote 6213
 process-interface-status
 commit
//The WTR time is not configured for BFD.
#
bfd eth-trunk3-2 bind peer-ip default-ip interface GigabitEthernet4/0/0
 discriminator local 6013
 discriminator remote 6213
 process-interface-status
 commit
//The WTR time is not configured for BFD.
#
```

Recovery measures:

Configure Eth-Trunk 1, Eth-Trunk 2, and Eth-Trunk 3 to work in static LACP mode or bind Eth-Trunk 2's and Eth-Trunk 3's member interfaces to BFD sessions.

- Configure Eth-Trunk interfaces to work in static LACP mode.

  # Configure Eth-Trunk 1.

  ```
  <HUAWEI> system-view
  [HUAWEI] interface eth-trunk 1
  [HUAWEI-Eth-Trunk1] mode lacp-static
  [HUAWEI-Eth-Trunk1] quit
  ```

  # Configure Eth-Trunk 2.


```
[HUAWEI] interface eth-trunk 2
[HUAWEI-Eth-Trunk2] mode lacp-static
[HUAWEI-Eth-Trunk2] quit
```

Configure Eth-Trunk 3.

```
[HUAWEI] interface eth-trunk 3
[HUAWEI-Eth-Trunk3] mode lacp-static
```

- Bind Eth-Trunk member interfaces to BFD sessions.

  # Bind Eth-Trunk 2's member interfaces to a BFD session.

```
<HUAWEI> system-view
[HUAWEI] bfd eth-trunk2-1 bind peer-ip default-ip interface
GigabitEthernet1/0/0
[HUAWEI-bfd-session-eth-trunk2-1] wtr 10
[HUAWEI-bfd-session-eth-trunk2-1] process-interface-status
[HUAWEI-bfd-session-eth-trunk2-1] quit
[HUAWEI] bfd eth-trunk2-2 bind peer-ip default-ip interface
GigabitEthernet3/0/0
[HUAWEI-bfd-session-eth-trunk2-2] wtr 10
[HUAWEI-bfd-session-eth-trunk2-2] process-interface-status
```

  # Bind Eth-Trunk 3's member interfaces to a BFD session.

```
<HUAWEI> system-view
[HUAWEI] bfd reth-trunk3-1 bind peer-ip default-ip interface
GigabitEthernet2/0/0
[HUAWEI-bfd-session-eth-trunk3-1] wtr 10
[HUAWEI-bfd-session-eth-trunk3-1] process-interface-status
[HUAWEI-bfd-session-eth-trunk3-1] quit
[HUAWEI] bfd eth-trunk3-2 bind peer-ip default-ip interface
GigabitEthernet4/0/0
[HUAWEI-bfd-session-eth-trunk3-2] wtr 10
[HUAWEI-bfd-session-eth-trunk3-2] process-interface-status
```

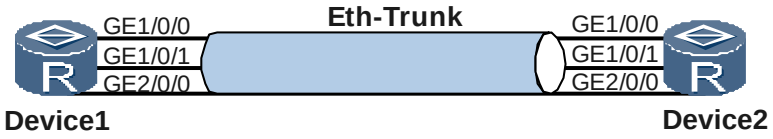
1.5.2.3 Add Interconnected Interfaces of Two Devices to Eth-Trunk Interfaces

When interfaces of one device are added to an Eth-Trunk interface, the interconnected interfaces of the other device must also be added to an Eth-Trunk interface. Otherwise, traffic is interrupted.

Scenario

Two routers are directly connected through three GE interfaces. The GE interfaces are bundled into an Eth-Trunk interface to increase available bandwidth and improve reliability.

Figure 1-7 Eth-Trunk usage scenario



Configuration Requirements

Interconnected interfaces of two devices that have Eth-Trunk interfaces configured must all be added to the Eth-Trunk interfaces.

Misconfiguration Risks

Risk description:

If only interfaces of one device are added to the Eth-Trunk interface, traffic could be interrupted between the two devices. The reason is as follows:

The device whose interfaces are all added to the Eth-Trunk interface balances traffic among all its member interfaces during traffic forwarding. However, the peer interfaces cannot receive or forward the traffic because they are not added to the Eth-Trunk interface.

Identification method:

Check whether the interconnected interfaces of the two devices are all added to the Eth-Trunk interfaces.

The following command output shows that Device 1's interfaces are added to Eth-Trunk 10, whereas Device 2 only has one interface added to Eth-Trunk 10, indicating that a risk exists.

```
<Device1> display eth-trunk 10
Eth-Trunk10's state information is:
WorkingMode: NORMAL       Hash arithmetic: According to flow
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 16
Operate status: up        Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
PortName                  Status     Weight
GigabitEthernet1/0/0        Up         1
GigabitEthernet1/0/1        Up         1
GigabitEthernet2/0/0        Up         1
<Device2> display eth-trunk 10
Eth-Trunk10's state information is:
WorkingMode: NORMAL       Hash arithmetic: According to flow
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 16
Operate status: up        Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
PortName                  Status     Weight
GigabitEthernet1/0/0        Up         1
```

Recovery measures:

Add the interconnected interfaces to the Eth-Trunk interface.

```
<Device2> system-view
[Device2] interface GigabitEthernet1/0/1
[Device2-GigabitEthernet1/0/1] eth-trunk 10
[Device2-GigabitEthernet1/0/1] quit
[Device2] interface GigabitEthernet2/0/0
[Device2-GigabitEthernet2/0/0] eth-trunk 10
[Device2-GigabitEthernet2/0/0] quit
```


1.5.3 IP-Trunk Configuration Instructions

1.1.1.1 Bind IP-Trunk Member Interfaces to BFD Sessions

IP-Trunk member interfaces must be bound to BFD sessions. Otherwise, failed links cannot be immediately detected.

Scenario

IP-Trunk interfaces are configured on devices.

Configuration Requirements

IP-Trunk member interfaces must be bound to BFD sessions.

NOTE
Configuring WTR time for BFD sessions is recommended.

Misconfiguration Risks

Risk description:

If IP-Trunk member interfaces are not bound to BFD sessions, IP-Trunk member link failures cannot be detected in real time, and services cannot be switched immediately.

When IP-Trunk member interfaces are bound to BFD sessions but delayed BFD switchback (WTR time) is not configured, BFD sessions frequently flap, causing the IP-Trunk member interfaces to frequently flap and affecting service convergence.

Identification method:

Check whether all the IP-Trunk member interfaces are bound to BFD sessions. The following command output shows that:

- IP-Trunk 1's member interface POS 1/0/0 is bound to a BFD session and has the WTR time configured.
- IP-Trunk 1's member interface POS 1/0/1 is bound to a BFD session but does not have the WTR time configured.
- IP-Trunk 2's two member interfaces are not bound to BFD sessions.

Therefore, both IP-Trunk 1 and IP-Trunk 2 have the problem described in this topic.

Check IP-Trunk member interfaces.

```
<HUAWEI> display interface ip-trunk 1
Ip-Trunk1 current state : DOWN
Line protocol current state : DOWN
Link quality grade : --
Description:HUAWEI, Ip-Trunk1 Interface
Route Port,Hash arithmetic : According to flow,Maximal BW: 311M,
Current BW: 0M,
 The Maximum Transmit Unit is 4470
Internet protocol processing : disabled Link layer protocol is
nonstandard HDLC
Physical is IP TRUNK
Current system time: 2017-03-28 17:10:01-08:00
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
```



```
   Last 300 seconds output rate 0 bits/sec, 0 packets/sec
   Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec
   Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec
   Input: 0 packets,0 bytes
         0 unicast,0 broadcast,0 multicast
         0 errors,0 unknownprotocol
   Output:0 packets,0 bytes
         0 unicast,0 broadcast,0 multicast
         0 errors
   Input bandwidth utilization  :   0%
   Output bandwidth utilization :   0%
------------------------------------------------------
PortName                  Status     Weight
------------------------------------------------------
Pos1/0/0                  DOWN       1
Pos1/0/1                  DOWN       1
------------------------------------------------------

<HUAWEI> display interface ip-trunk 2
Ip-Trunk2 current state : DOWN
Line protocol current state : DOWN
Link quality grade : --
Description:HUAWEI, Ip-Trunk2 Interface
Route Port,Hash arithmetic : According to flow,Maximal BW: 311M,
Current BW: 0M,
 The Maximum Transmit Unit is 4470
Internet protocol processing : disabled Link layer protocol is
nonstandard HDLC
Physical is IP TRUNK
Current system time: 2017-03-28 17:15:51-08:00
   Last 300 seconds input rate 0 bits/sec, 0 packets/sec
   Last 300 seconds output rate 0 bits/sec, 0 packets/sec
   Realtime 99 seconds input rate 0 bits/sec, 0 packets/sec
   Realtime 99 seconds output rate 0 bits/sec, 0 packets/sec
   Input: 0 packets,0 bytes
         0 unicast,0 broadcast,0 multicast
         0 errors,0 unknownprotocol
   Output:0 packets,0 bytes
         0 unicast,0 broadcast,0 multicast
         0 errors
   Input bandwidth utilization  :   0%
   Output bandwidth utilization :   0%
------------------------------------------------------
PortName                  Status     Weight
------------------------------------------------------
Pos1/0/2                  DOWN       1
Pos1/0/3                  DOWN       1
------------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 0
```

Check whether all the IP-Trunk member interfaces are bound to BFD sessions.

```
<HUAWEI> display current-configuration configuration bfd-session
#
bfd BFD-IPtrunk1-1 bind peer-ip default-ip interface Pos1/0/0
```



```
 discriminator local 6013
 discriminator remote 6213
 wtr 10
 process-interface-status
 commit
#
//IP-Trunk member interface POS 1/0/0 is bound to a BFD session and has a WTR time configured.
bfd BFD-IPtrunk1-2 bind peer-ip default-ip interface Pos1/0/1
 discriminator local 6010
 discriminator remote 6213
 process-interface-status
 commit
#
//IP-Trunk member interface POS 1/0/1 does not have a WTR time configured
//IP-Trunk 2's member interfaces POS 1/0/2 and POS 1/0/3 are not bound to BFD sessions
return
```

Recovery measures:

Bind IP-Trunk member interfaces to BFD sessions and configure a WTR time for BFD sessions.

- Bind IP-Trunk 1's member interface POS 1/0/1 to a BFD session and configure a WTR time for the BFD session.

```
<HUAWEI> system-view
[HUAWEI] bfd BFD-IPtrunk1-2
[HUAWEI-bfd-session-BFD-IPtrunk1-2] wtr 10
```

- Bind IP-Trunk 2's member interfaces POS 1/0/2 and POS 1/0/3 to BFD sessions and configure a WTR time for the BFD sessions.

```
<HUAWEI> system-view
[HUAWEI] bfd BFD-Iptrunk2-1 bind peer-ip default-ip interface
Pos1/0/2
[HUAWEI-bfd-session-BFD-Iptrunk2-1] discriminator local 6000
[HUAWEI-bfd-session-BFD-Iptrunk2-1] discriminator remote 6001
[HUAWEI-bfd-session-BFD-Iptrunk2-1] wtr 10
[HUAWEI-bfd-session-BFD-Iptrunk2-1] process-interface-status
[HUAWEI-bfd-session-BFD-Iptrunk2-1] commit
[HUAWEI-bfd-session-BFD-Iptrunk2-1] quit
[HUAWEI] bfd BFD-Iptrunk2-2 bind peer-ip default-ip interface
Pos1/0/3
[HUAWEI-bfd-session-BFD-Iptrunk2-2] discriminator local 6002
[HUAWEI-bfd-session-BFD-Iptrunk2-2] discriminator remote 6003
[HUAWEI-bfd-session-BFD-Iptrunk2-2] wtr 10
[HUAWEI-bfd-session-BFD-Iptrunk2-2] process-interface-status
[HUAWEI-bfd-session-BFD-Iptrunk2-2] commit
```


1.6 IP Routing

1.6.1 Common IGP Configuration Instructions

1.1.1.1 Configure an Appropriate IGP Neighbor Dead Interval

If the IGP (OSPF or IS-IS) neighbor dead interval is too short, neighbor relationships may easily go down, interrupting services.

Scenario

An IGP, such as OSPF or IS-IS, is configured.

Configuration Requirements

Using the default neighbor dead interval is recommended.

Misconfiguration Risks

Risk description:

If either the OSPF or IS-IS neighbor dead interval is too short, neighbor relationships may easily go down, interrupting services.

- On an IS-IS interface, if the **isis timer hello 3** command is run but the **isis timer holding-multiplier** *number* command is not, the neighbor dead interval is considered too short.
- On an OSPF interface, the neighbor dead interval is considered too short if either of the following conditions is met:
  - The **ospf timer hello 1** command is run, but the **ospf timer dead** *interval* command is not.
  - The **ospf timer dead** *interval* command is run, and the value of *interval* is not greater than 4.

Identification method:

1. Check whether OSPF or IS-IS is enabled.

   # Run the **display current-configuration configuration isis** or **display current-configuration configuration ospf** commands in any view to check whether IS-IS or OSPF configuration is displayed.

```
<HUAWEI> display current-configuration configuration isis
#
isis 100
 is-level level-2
 cost-style wide
 network-entity 10.0000.0100.0005.00
#
<HUAWEI> display current-configuration configuration ospf
#
ospf 100
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.3.3.0 0.0.0.255
```



```
#
```

2. Check the interfaces on which OSPF or IS-IS is enabled.

   # Run the **display isis interface verbose** command in any view to check IS-IS-enabled interfaces. In the following example, GE 3/0/6.1001 is an IS-IS-enabled interface.

```
<HUAWEI> display isis interface verbose
                  Interface information for ISIS(100)
                  ------------------------------------
 Interface      Id     IPV4.State        IPV6.State     MTU  Type  DIS
 GE3/0/6.1001   001       Up              Down       1497 L1/L2 --
  Circuit MT State          : Standard
  Circuit Parameters        : p2p
  Description              : HUAWEI, GigabitEthernet3/0/6.1001 Interface
  SNPA Address             : 0018-8266-56be
  IP Address               : 10.1.1.5
  IPV6 Link Local Address    :
  IPV6 Global Address(es)    :
  Csnp Timer Value          :  L12   10
  Hello Timer Value         :       10
  DIS Hello Timer Value      :
  Hello Multiplier Value     :     1000
  LSP-Throttle Timer        :  L12   50
  Cost                     :  L1    10  L2    10
  Ipv6 Cost                :  L1    10  L2    10
  Retransmit Timer Value     :  L12    5
  Bandwidth-Value           :  Low 1000000000  High        0
  Static Bfd               :  NO
  Dynamic Bfd              :  NO
  Dynamic IPv6 Bfd          :  NO
  Fast-Sense Rpr           :  NO
  Extended-Circuit-Id Value   :  0000000001
  Suppress Base            :  NO
  IPv6 Suppress Base        :  NO
  Link quality adjust cost    :  NO
Link quality             :  0x0(Best)
```

   # Run the **display ospf interface all** command in any view to check OSPF-enabled interfaces. In the following example, GE 3/0/4 and GE 3/0/9 are OSPF-enabled interfaces.

```
<HUAWEI> display ospf interface all
       OSPF Process 100 with Router ID 10.1.1.2
             Interfaces
 Area: 0.0.0.0        (MPLS TE not enabled)
```

```
 Interface: 10.3.3.1 (GigabitEthernet3/0/4)
```

```
 Cost: 1      State: BDR      Type: Broadcast    MTU: 1500
 Priority: 1
 Designated Router: 10.3.3.2
 Backup Designated Router: 10.3.3.1
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1
 Interface: 310.1.1.1 (GigabitEthernet3/0/9)
 Cost: 1      State: DR       Type: Broadcast    MTU: 1500
 Priority: 1
 Designated Router: 310.1.1.1
 Backup Designated Router: 310.1.1.2
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1
```


3. Check whether the neighbor dead interval is too short.

   On an IS-IS interface, if the **isis timer hello 3** command is run but the **isis timer holding-multiplier** *number* command is not, the neighbor dead interval is considered too short.

   On an OSPF interface, the neighbor dead interval is considered too short if either of the following conditions is met:

   - The **ospf timer hello 1** command is run but the **ospf timer dead** *interval* command is not.
   - The **ospf timer dead** *interval* command is run, and the value of *interval* is not greater than 4.

   # Check the configuration of an IS-IS-enabled interface (GE 3/0/6.1001 in this example). In the following example, the neighbor dead interval is too short.

```
<HUAWEI> display current-configuration interface GigabitEthernet3/0/6.1001
#
interface GigabitEthernet3/0/6.1001
 vlan-type dot1q 1001
 ip address 10.1.1.5 255.255.255.0
 isis enable 100
 isis circuit-type p2p
 isis timer hello 3
#
return
```

   # Check the configuration of an OSPF-enabled interface (GE 3/0/4 in this example). The following command output shows that the neighbor dead interval is too short.

```
<HUAWEI> display current-configuration interface GigabitEthernet3/0/4
#
interface GigabitEthernet3/0/4
 undo shutdown
 ip address 10.3.3.1 255.255.255.0
 ospf timer hello 1
#
return
```

   # Check the configuration of an OSPF-enabled interface (GE 3/0/9 in this example). The following command output shows that the neighbor dead interval is too short.

```
<HUAWEI> display current-configuration interface GigabitEthernet3/0/9
#
interface GigabitEthernet3/0/9
 undo shutdown
 ip address 310.1.1.1 255.255.255.0
 ospf timer hello 3
 ospf timer dead 4
#
return
```

Recovery measures:

Use the default neighbor dead interval.

1.6.1.2 Configure a Higher Priority for Routes Imported by an IGP Than Routes Generated by the IGP

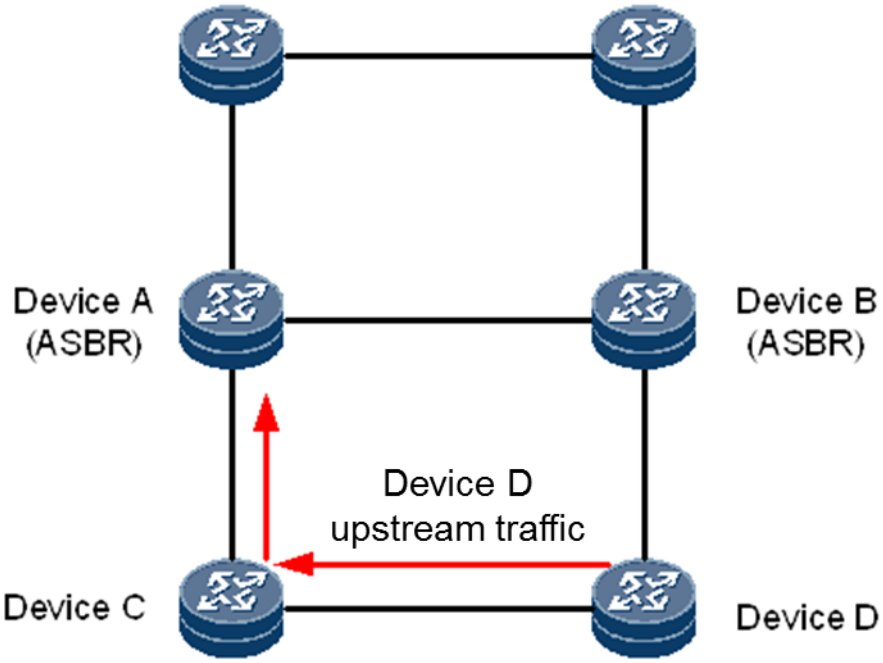
Multiple ASBRs are enabled to use an IGP to import external routes. If the priority of imported routes is lower than that of the routes generated by the IGP, only one ASBR can

import external routes using the IGP, and all the other ASBRs can only learn the external routes from that ASBR. As a result, upstream traffic will bypass these ASBRs that cannot directly import the external routes.

Scenario

In Figure 1-8, Device A and Device B are ASBRs and are enabled to import BGP routes using OSPF. To guide upstream traffic forwarding, Device A advertises the imported routes to Device C, and Device B advertises the imported routes to Device D. Device B also learns the OSPF routes from Device A, and then the BGP routes on Device B become inactive because the priority of BGP routes is lower than that of OSPF routes. As a result, Device B does not advertise the BGP routes to Device D. In this case, upstream traffic of Device D bypasses Device B and flows to Device A through Device C.

Figure 1-8 Unexpected traffic bypass because IGP routes take precedence over imported routes



Configuration Requirements

The priority value of IGP routes must be larger than that of imported routes. The larger the value, the lower the priority.

NOTE
Ensure that services are not affected when the priority value of IGP routes is changed.

Misconfiguration Risks

Risk description:

Upstream traffic flows through the same ASBR and then is forwarded using the original routes if the following conditions are met:

1 Multiple ASBRs are configured to use an IGP to import routes from a different protocol.

2. The priority of the imported routes is lower than that of IGP routes.

Identification method:

1 Check whether an IGP is configured to import routes from a different protocol.

Run the **display current-configuration configuration ospf** command in any view to check whether OSPF is configured to import routes from a different protocol. The following command output shows that BGP routes are imported by OSPF.

```
<HUAWEI> display current-configuration configuration ospf
#
ospf 1 router-id 10.1.1.6
 import-route bgp
 area 0.0.0.0
  network 10.1.19.6 0.0.0.0
#
return
```

Run the **display current-configuration configuration ospfv3** command in any view to check whether OSPFv3 is configured to import routes from a different protocol. The following command output shows that static routes are imported by OSPFv3.

```
<HUAWEI> display current-configuration configuration ospfv3
#
ospfv3 1
 router-id 10.1.1.1
 import-route static
#
return
```

Run the **display current-configuration configuration isis** command in any view to check whether IS-IS is configured to import routes from a different protocol. The following command output shows that static routes are imported by IS-IS.

```
<HUAWEI> display current-configuration configuration isis
#
isis 1
 cost-style wide
 network-entity 10.000a.0011.0006.00
 import-route static
#
return
```

3. Check the priority of the imported routes.

Check OSPF configurations. The following command output shows that the priority of OSPF intra-area, inter-area, ASE, and NSSA routes is 200.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] display this
#
ospf 1
 preference 200
 preference ase 200
#
return
```

Check OSPFv3 configurations. The following command output shows that the priority of OSPFv3 intra-area, inter-area, ASE, and NSSA routes is 100.

```
<HUAWEI> system-view
```



```
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] display this
#
ospfv3 1
 router-id 10.1.19.6
 preference 100
 preference ase 100
#
return
```

Check IS-IS configurations. The following command output shows that the priority of IS-IS intra-area and inter-area routes is 200.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1]  display this
#
isis 1
 cost-style wide
 network-entity 00.0005.0000.0019.0006.00
 preference 200
#
return
```

Check BGP configurations. The following command output shows that the priorities of EBGP, IBGP, and local routes are 200, 180, and 150, respectively.

```
<HUAWEI> system-view
[HUAWEI] bgp
[HUAWEI-bgp] display this
#
bgp 100
 #
 ipv4-family unicast
  undo synchronization
  preference 200 180 150
#
```

Check RIP configurations. The following command output shows that the priority of RIP routes is 200.

```
<HUAWEI> display current-configuration configuration rip
#
rip 1
 preference 200
#
return
```

Check RIPng configurations. The following command output shows that the priority of RIPng routes is 200.

```
<HUAWEI> display current-configuration configuration ripng
#
ripng 1
 preference 200
#
return
```

Check static route configurations. The following command output shows that the priority of static routes is 200.

```
<HUAWEI> display current-configuration configuration
```



```
#
 ……
ip route-static 10.1.1.1 32 NULL 0 preference 200
#
```

4. If no route priority is configured, Huawei devices use the following default priorities:

Route Type	Priority Defined by Huawei
Direct	0
OSPF	10
IS-IS	15
Static	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
IBGP	255
EBGP	255
BGP Local	255

Recovery measures:

Reduce the priority value of IGP routes to a value smaller than that of imported routes using the **preference** command. The smaller the value, the higher the priority.

1.6.2 OSPF Configuration Instructions

1.1.1.1 Configure the Same Network Type on Local and Remote OSPF Interfaces

If the network types of two interfaces are different (for example, P2P on one end and broadcast on the other end), they can set up a neighbor relationship, but cannot learn routes from each other.

Scenario

OSPF is enabled on two interfaces.

Configuration Requirements

The network types must be the same for a local and its neighbor OSPF interfaces.

Misconfiguration Risks

Risk description:

If the network types of two interfaces are different (for example, P2P on one end and broadcast on the other end), they can set up a neighbor relationship, but cannot learn routes from each other. When this is the case, some services will be interrupted.

Identification method:

1. Run the **display ospf interface all** command in the user view to check detailed information about OSPF interfaces.

   The following command output shows that two OSPF broadcast interfaces (GE 1/0/1 and GE 1/1/0) have established a neighbor relationship.

```
<HUAWEI> display ospf interface all
       OSPF Process 101 with Router ID 10.1.1.1
              Interfaces

 Area: 0.0.0.0        (MPLS TE not enabled)

 Interface: 192.168.1.1 (GigabitEthernet1/0/1)
 Cost: 1      State: DROther   Type: Broadcast   MTU: 1500  Priority: 123
 Designated Router: 192.168.1.3
 Backup Designated Router: 0.0.0.0
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1

 Interface: 192.168.2.1 (GigabitEthernet1/1/0)
 Cost: 1      State: DROther   Type: Broadcast   MTU: 1500
 Priority: 0
 Designated Router: 192.168.2.3
 Backup Designated Router: 0.0.0.0
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1
```

2. Run the **display ospf peer** *interface-name* command in the user view to check OSPF neighbors on each interface.

   Check the command output. If an interface has no OSPF neighbor relationships or its neighbor relationships are not in the Full state, check OSPF neighbor relationships of other interfaces. If an OSPF neighbor relationship is in the Full state, check whether the network types are the same on both ends.

NOTE

- For broadcast neighbors, if the **DR** field value is an IP address, the network types are the same. If its value is **None**, the network types are different.
- For P2P neighbors, if the **DR** field value is **None**, the network types are the same. If any other value is displayed, the network types are different.

   In the following example, the broadcast interface GE 1/0/1's neighbor relationship is in the Full state, but no IP address is displayed in the **DR** field. This indicates that the network types of the local and neighbor interfaces are different.

```
<HUAWEI> display ospf peer GigabitEthernet1/0/1
      OSPF Process 101 with Router ID 10.1.1.1
             Neighbors

 Area 0.0.0.0 interface 192.168.1.1(GigabitEthernet1/0/1)'s neighbors
 Router ID: 10.1.1.3   Address: 192.168.1.3
   State: Full  Mode:Nbr is  Master  Priority: 123
   DR: None   BDR: None   MTU: 0
   Dead timer due in 33  sec
   Retrans timer interval: 5
   Neighbor is up for 00:45:35
   Authentication Sequence: [ 0 ]
```



```
<HUAWEI> display ospf peer GigabitEthernet1/1/0

       OSPF Process 101 with Router ID 10.1.1.1
              Neighbors

 Area 0.0.0.0 interface 192.168.2.1(GigabitEthernet1/1/0)'s neighbors
 Router ID: 10.1.1.3   Address: 192.168.2.3
   State: Full  Mode:Nbr is  Master  Priority: 1
DR: 192.168.2.3  BDR: None   MTU: 0       Dead timer due in 32  sec
   Retrans timer interval: 5
   Neighbor is up for 00:23:12
   Authentication Sequence: [ 0 ]
```

Recovery measures:

Run the **ospf network-type** command in the view of the local or neighbor interface to modify the network type to be the same as that configured on the other end.

1 The following command output shows that the network type of GE 1/0/1 has been changed to P2P.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet1/0/1
[HUAWEI-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 192.168.1.1 255.255.255.0
 ospf network-type p2p
 ospf dr-priority 123
#
return
```

3. Run the **display ospf peer** *interface-name* command in the user views of both devices to check the **DR** field.

   In the following example, an IP address is displayed in the DR field of GE 1/0/1's OSPF neighbor relationship, indicating that the network types of the local and neighbor interfaces are the same.

```
<HUAWEI> display ospf peer GigabitEthernet1/0/1
       OSPF Process 101 with Router ID 10.1.1.1
              Neighbors

 Area 0.0.0.0 interface 192.168.1.1(GigabitEthernet1/0/1)'s neighbors
 Router ID: 10.1.1.3   Address: 192.168.1.3
   State: Full  Mode:Nbr is  Master  Priority: 123
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 38  sec
   Retrans timer interval: 5
   Neighbor is up for 00:00:07
   Authentication Sequence: [ 0 ]
```


1.6.3 IS-IS Configuration Instructions

1.1.1.1 Disable Default Route Advertisement Before a Cutover

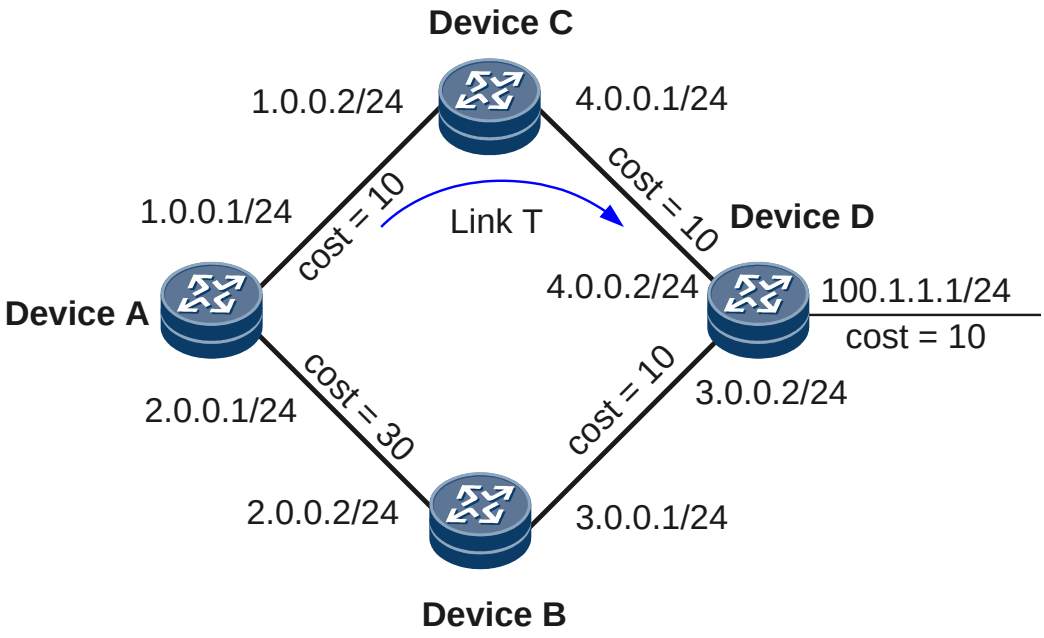
If a device sets the overload (OL) bit to 1 in IS-IS LSPs, the routes passing through the device are switched to a backup path. If the device is enabled to advertise its default route, the default route is not switched to the backup path.

Scenario

In Figure 1-9, IS-IS neighbor relationships are established between Device A, Device B, Device C, and Device D. The primary path passes through Device A, Device C, and Device D, and the backup path passes through Device A, Device B, and Device D. The problem may occur in either of the following scenarios:

- The **set-overload** command is run in the IS-IS process view on Device C to switch services immediately to the backup path in a cutover scenario.
- The **set-overload on-startup** command is run in the IS-IS process view on Device C to delay route switchback in case of a master/slave main control board switchover or device restart.

Figure 1-9 Failure of the default route to be switched to the backup path after the OL bit is set to 1



Configuration Requirements

Default route advertisement must be disabled in the IS-IS process view before a cutover and then re-enabled after the cutover.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] undo default-route-advertise
```

Misconfiguration Risks

Risk description:

If the **set-overload on-startup** and **default-route-advertise** commands are run in the IS-IS process view on Device C, the default route is not switched to the backup path during the cutover. If no specific routes are available, services are interrupted.

Specifically, after the timer (600s by default) that starts upon a device restart or master/slave main control board switchover expires, the default route is not switched to the backup path.

Identification method:

Run the **display isis** *process-id* **lsdb local verbose** command in any view to check LSP information. If the OL bit is 1 and default route advertisement is enabled, the problem has occurred. In the following example, the OL bit is 1, and default route advertisement is enabled.

```
<HUAWEI> display isis 1 lsdb local verbose
       ATTENTION: System is overloaded
       Manual overload set    YES    OverLoad on Startup    NO
       System Memory Low      NO     Memory Allocate Failure NO
                      Level-2 Link State Database
LSPID            Seq Num    Checksum    Holdtime     Length  ATT/P/OL
--------------------------------------------------------------------------------
abcd.0001.0031.00-00* 0x0000008e   0x6726       1183         76     0/0/1
 SOURCE      abcd.0001.0031.00
 NLPID       IPV4
 AREA ADDR   10
 INTF ADDR   10.10.1.1
 INTF ADDR   10.1.1.2
+NBR  ID     aaaa.0001.0030.00  COST: 10
+IP-Extended  10.10.1.1     255.255.255.255  COST: 0
+IP-Extended  10.1.1.0      255.255.255.0    COST: 10
abcd.0001.0031.00-01* 0x00000001   0x289a       1179         34     0/0/0
 SOURCE      abcd.0001.0031.00
+IP-Extended  0.0.0.0       0.0.0.0         COST: 0
   *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
         ATT-Attached, P-Partition, OL-Overload
```

Recovery measures:

Run the **undo default-route-advertise** command in the IS-IS process view before a cutover, and run the **default-route-advertise** command after the cutover.

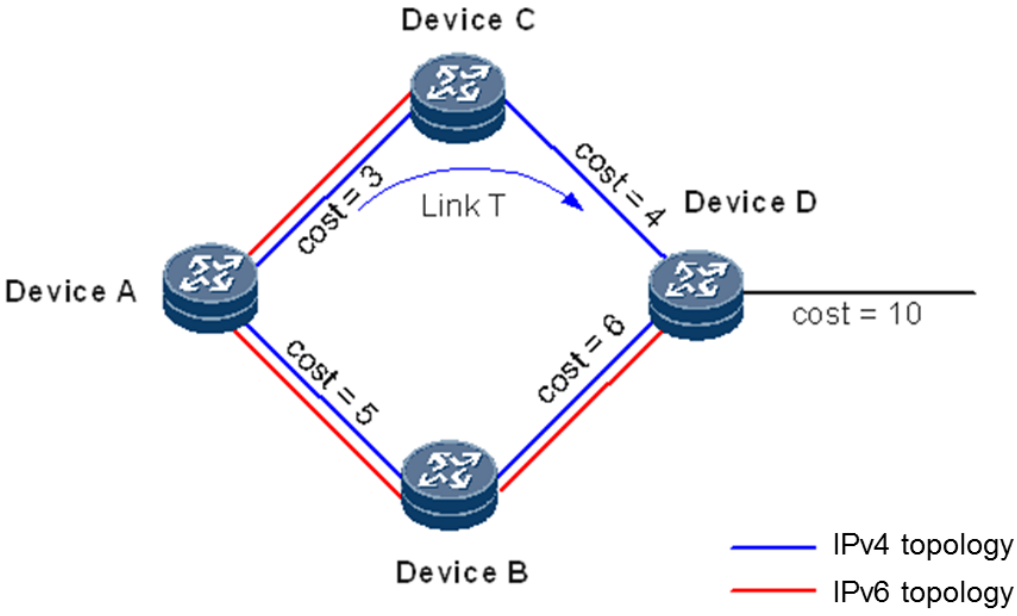
1.6.3.2 Enable IPv6 for an Interface That Uses the Standard IS-IS IPv6 Topology

In an IS-IS IPv6 standard topology, IPv4 and IPv6 services share the same shortest path tree (SPT). If an outbound interface of a device on the SPT does not support IPv6, an IPv6 blackhole route is generated on the device, or a routing loop occurs. As a result, IPv6 services are interrupted.

Scenario

In Figure 1-10, IS-IS neighbor relationships are established between Device A, Device B, Device C, and Device D. IS-IS is deployed for IPv4 and IPv6 services. The standard IS-IS IPv6 topology is used.

Figure 1-10 IPv6 service interruption due to a lack of an independent IPv6 topology



Configuration Requirements

IPv6 services must use an independent IS-IS IPv6 topology so that IPv6 SPT calculation can be isolated from IPv4 SPT calculation.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] display this
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0001.00
 #
 ipv6 enable topology ipv6
 #
#
return
```

Misconfiguration Risks

Risk description:

An IPv6 blackhole route is generated on a device or a routing loop occurs if IPv6 is enabled for an IS-IS process using the **ipv6 enable topology standard** command, the standard

topology mode is specified, and an outbound interface of the device on the SPT does not support IPv6. When this is the case, IPv6 services will be interrupted.

Identification method:

1 Run the **display current-configuration configuration isis** command in any view to check whether the standard topology mode is specified in the IS-IS process.

```
<HUAWEI> display current-configuration configuration isis
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0001.00
 #
 ipv6 enable topology standard
 #
#
return
```

2. Run the **display isis** *process-id* **interface verbose** command in any view to check the IS-IS interface status and topology type and check whether there are interfaces with **IPV4.State**, **IPV6.State**, and **Circuit MT State** being **UP**, **Down**, and **Standard**, respectively. In the following example, GE 1/0/0.1 is such an interface.

```
<HUAWEI> display isis 1001 interface verbose
                 Interface information for ISIS(1001)
                 ------------------------------------
 Interface      Id     IPV4.State         IPV6.State     MTU  Type  DIS
 GE1/0/0.1   001       Up              Down        1497 L1/L2 --
  Circuit MT State          : Standard
  Circuit Parameters        : p2p
  Description              : HUAWEI, GigabitEthernet1/0/0.1 Interface
  SNPA Address             : 781d-ba56-fa3a
  IP Address               : 10.1.1.6
  IPV6 Link Local Address    :
  IPV6 Global Address(es)    :
  Csnp Timer Value          :  L12   10
  Hello Timer Value         :       10
  DIS Hello Timer Value      :
  ……
```

3. Run the **display current-configuration configuration interface** *interface-name* command in any view to check whether IPv6 is enabled on the interface. The following command output shows that the **isis ipv6 enable** command is not run for GE1/0/0.1. In this case, the problem may occur.

```
<HUAWEI> display current-configuration interface GigabitEthernet1/0/0.1
#
interface GigabitEthernet1/0/0.1
 ip address 10.2.0.1 255.255.255.0
 isis enable 1
 isis circuit-type p2p
#
```

Recovery measures:

Enable IPv6 on an interface.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet1/0/0.1
```



```
[HUAWEI-interface-GigabitEthernet1/0/0.1] display this
#
interface GigabitEthernet1/0/0.1
 ipv6 enable
 ip address 10.2.0.1 255.255.255.0
 ipv6 address auto link-local
 isis enable 1
 isis ipv6 enable 1
 isis circuit-type p2p
#
```

1.6.4 BGP Configuration Instructions

1.1.1.1 Configure a Priority for BGP Routes Properly

A local device sends its static route to a remote device through OSPF. The remote device imports the route to BGP as a BGP route and advertises the BGP route to the local device. If the **preference** command is run on the local device to allow BGP routes to have a higher priority than static routes, route flapping occurs.

Scenario

On the network shown in Figure 1-11:

1. Router A imports a static route to its OSPF routing table as an OSPF route and sends the OSPF route to Router B.
2. Router B imports the OSPF route to its BGP routing table as a BGP route and advertises the BGP route to Router A.
3. If the **preference** command is run in the BGP view on Router A to allow BGP routes to have a higher priority than static routes, the static route on Router A becomes inactive. Then OSPF deletes the route and notifies Router B of the deletion of the route.
4. Router B deletes the corresponding BGP route and notifies Router A of the deletion of the route. Router A then deletes the BGP route from its routing table. Then the static route on Router A becomes active again. Consequently, OSPF imports the static route again, causing circular processing. As a result, route flapping occurs.

Figure 1-11 BGP route flapping

Configuration Requirements

The priority of BGP routes must be lower than that of static routes.

Misconfiguration Risks

Risk description:

An OSPF neighbor relationship and a BGP peer relationship are configured between Router A and Router B. A static route is configured on Router A and imported to the OSPF routing table. Router B imports the route to its BGP routing table through the **import-route** or **network** command. If the **preference** command is run in the BGP view on Router A to allow BGP routes to have a higher priority than static routes, route flapping occurs, affecting services.

Identification method:

1 Display the IP routing table on Router A repeatedly to check whether the protocol of the route destined for the destination IP address of the static route alternates between static and BGP. The destination IP address 10.0.0.0 is used in the following example:

```
<HUAWEI> display ip routing-table 10.0.0.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination: 10.0.0.0/8
    Protocol: Static         Process ID: 0
  Preference: 60                 Cost: 0
     NextHop: 0.0.0.0         Neighbour: 0.0.0.0
       State: Active Adv           Age: 04h36m27s
         Tag: 0               Priority: medium
       Label: NULL             QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0         Interface: NULL0
    TunnelID: 0x0                Flags:  D
<HUAWEI> display ip routing-table 10.0.0.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 2
Destination: 10.0.0.0/8
    Protocol: IBGP           Process ID: 0
  Preference: 20                 Cost: 1
     NextHop: 10.1.0.4       Neighbour: 10.1.0.4
       State: Active Adv Relied      Age: 00h00m00s
         Tag: 0               Priority: low
       Label: NULL             QoSInfo: 0x0
  IndirectID: 0x1ee
 RelayNextHop: 0.0.0.0         Interface: Vlanif503
    TunnelID: 0x0                Flags: RD
Destination: 10.0.0.0/8
    Protocol: Static         Process ID: 0
  Preference: 60                 Cost: 0
     NextHop: 0.0.0.0         Neighbour: 0.0.0.0
       State: Inactive Adv          Age: 04h36m28s
         Tag: 0               Priority: medium
       Label: NULL             QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0         Interface: NULL0
    TunnelID: 0x0                Flags:
```


5. Display the IP routing table on Router B repeatedly. It turns out that route flapping occurs too.

```
<HUAWEI> display ip routing-table 10.0.0.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination: 10.0.0.0/8
    Protocol: O_ASE          Process ID: 20
  Preference: 150                Cost: 1
     NextHop: 10.1.0.3       Neighbour: 0.0.0.0
       State: Active Adv           Age: 00h00m14s
         Tag: 1               Priority: medium
       Label: NULL              QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0         Interface: Vlanif503
    TunnelID: 0x0                Flags:  D
<HUAWEI> display ip routing-table 10.0.0.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination: 10.0.0.0/8
    Protocol: O ASE          Process ID: 20
  Preference: 150                Cost: 1
     NextHop: 10.1.0.3       Neighbour: 0.0.0.0
       State: Active Adv           Age: 00h00m00s
         Tag: 1               Priority: medium
       Label: NULL              QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0         Interface: Vlanif503
    TunnelID: 0x0                Flags:  D
<HUAWEI> display ip routing-table 10.0.0.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination: 10.0.0.0/8
    Protocol: O ASE          Process ID: 20
  Preference: 150                Cost: 1
     NextHop: 10.1.0.3       Neighbour: 0.0.0.0
       State: Active Adv           Age: 00h00m01s
         Tag: 1               Priority: medium
       Label: NULL              QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0         Interface: Vlanif503
    TunnelID: 0x0                Flags:  D
```

Recovery measures:

Measure 1: Delete the **preference** configuration from the BGP public network IPv4 address family view on Router A.

Solution 2: Increase the priority of static routes to be higher than that of BGP routes. The smaller the preference value, the higher the priority.

1.7 IP Multicast

1.7.1 PIM Configuration Instructions

1.1.1.1 Enable PIM on All Interfaces Connected to Equal-Cost Links or Primary and Secondary Links

If equal-cost links or primary and secondary links are available for Layer 3 multicast services, PIM must be enabled on all interfaces that connect to the links. If PIM is not enabled on some interfaces, multicast services may be interrupted after a link switchover.

Scenario

Equal-cost links or primary and secondary links are available for multicast services.

Configuration Requirements

PIM must be enabled on all interfaces that connect to equal-cost links or primary and secondary links for Layer 3 multicast services.

Misconfiguration Risks

Risk description:

In a multicast scenario with equal-cost links or primary and secondary links, PIM is enabled only for the active link in use, but not enabled on the other links. After a link switchover is triggered by some causes, such as configuration, route, or link changes, multicast services will be interrupted, because PIM is not enabled for the newly selected link and PIM routes cannot be created for the new link.

Identification method:

Run the **display pim interface** command in the user view to check whether PIM is enabled on the interfaces that connect to equal-cost links or the primary and secondary links for multicast services.

If PIM configurations are displayed for a specified interface, PIM is enabled on the interface. Otherwise, PIM is disabled on the interface. The following command output indicates that PIM is enabled on Ethernet 1/0/0.

```
<HUAWEI> display pim interface Ethernet1/0/0
 VPN-Instance: public net
 Interface     State   NbrCnt   HelloInt   DR-Pri    DR-Address
 Ethernet1/0/0  up     1       30        1         10.1.1.1
```

Recovery measures:

Enable PIM in the views of the interfaces on which PIM is disabled.

1.8 MPLS

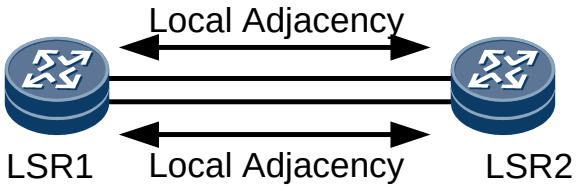
1.8.1 MPLS LDP Configuration Instructions

1.1.1.1 Configure the Same Parameters in Both the LDP Interface View and Remote LDP Peer View in a Multi-Link Scenario or for a Local and Remote Coexistence LDP Session

If multiple links exist or a local and remote coexistence LDP session is created between two LSRs, the LDP session can be established only over a single link or cannot be established.

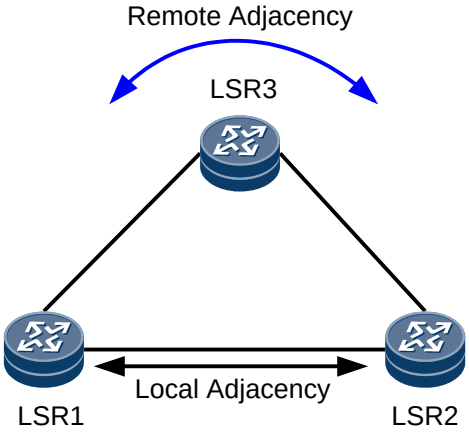
Scenario 1 — Multiple Links Between Two LSRs

Figure 1-12 LDP session only over a single link or LDP session failure with multiple links between LSRs



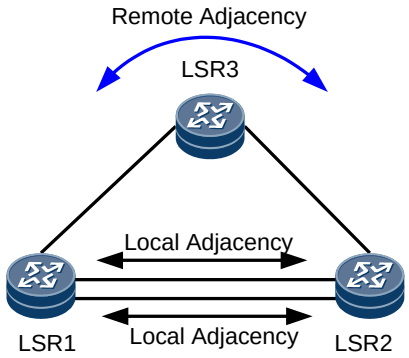
Scenario 2 — A Local and Remote Coexistence LDP Session Between Two LSRs

Figure 1-13 Local and remote coexistence LDP session created only over a single link or failing



Scenario 3 — Multiple Links and a Local and Remote Coexistence LDP Session Between Two LSRs

Figure 1-14 LDP session only over a single link or LDP session failure with a local and remote coexistence LDP session created and multiple links between LSRs



Configuration Requirements

In the preceding scenarios, parameters configured in the LDP interface view and remote LDP peer view must be the same. For the same LDP peer, one of the following commands is run in some local interface views and remote LDP peer view, or this command is run in all local interface views and remote LDP peer view but the configured parameters differ. In this situation, you must use the same or default parameter in the local interface views and remote LDP peer view in one of the following commands:

- **mpls ldp transport-address**
- **mpls ldp transport-address**
- **mpls ldp timer keepalive-hold**
- **mpls ldp timer keepalive-send**
- **mpls ldp advertisement**
- **mpls ldp local-lsr-id**

Misconfiguration Risks

Risk description:

Run the **display mpls ldp adjacency all** command in the user view. If LDP adjacencies with the same peer ID exist on the device, some sources of the LDP session cannot be bound to. As a result, load-balancing LDP LSPs or protection for the local and remote LDP sessions cannot be provided. In addition, if the LDP session fails to be created, services are interrupted.

Identification method:

1 Run the **display mpls ldp adjacency all c**ommand in any view and check information about LDP adjacencies. If no command output is displayed, this problem does not occur. Otherwise, continue the check.

In the following information, the information in bold indicates that the same peer ID is mapped to multiple links or a local and remote coexistence LDP session. In this example, the peer IDs are **10.1.1.2**, **10.1.1.3**, and **10.6.6.6**. Go to the next step.


```
<HUAWEI> display mpls ldp adjacency all
LDP Adjacency Information in Public Network
 Codes: R: Remote Adjacency, L: Local Adjacency
 A '*' before an adjacency means the adjacency is being deleted.
 ------------------------------------------------------------------------------
 SN   SourceAddr     PeerID      VrfID AdjAge(DDDD:HH:MM) RcvdHello Type
 ------------------------------------------------------------------------------
  1   10.2.2.1       10.1.1.2      0    0000:00:37       449      L
  2   10.2.1.1       10.1.1.4      0    0000:00:04       57       L
  3   10.1.1.2      10.1.1.2      0    0000:00:09       148      R
  4   10.3.3.3       10.1.1.2      0    0000:00:00       11       L
  5   10.2.3.1       10.1.1.3      0    0000:00:20       258      L
  6   10.1.1.2      10.1.1.3      0    0000:00:20       76       R
 ------------------------------------------------------------------------------
LDP Adjacency Information in VPN-Instance: vpn1
 Codes: R: Remote Adjacency, L: Local Adjacency
 A '*' before an adjacency means the adjacency is being deleted.
 ------------------------------------------------------------------------------
 SN   SourceAddr    PeerID       VrfID AdjAge(DDDD:HH:MM) RcvdHello Type
 ------------------------------------------------------------------------------
  1   10.3.2.1       10.6.6.6        1    0000:00:08       103      L
  2   10.4.2.1       10.6.6.6        1    0000:00:02       33       L
 ------------------------------------------------------------------------------
TOTAL: 8 Record(s) found.
```

2. Check for multiple adjacencies with the same peer ID.

   # If a local adjacency is configured, run the **display ip routing-table** *ip-address* command in any view and check outbound interface information. Peer ID 10.1.1.2 is used as an example. Two local adjacencies destined for **10.2.2.1** and **10.3.3.3** and a remote adjacency destined for **10.1.1.2** are created. For example:

```
<HUAWEI> display ip routing-table 10.2.2.1
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
10.2.2.1/32  Direct  0    0           D   127.0.0.1      GigabitEthernet1/0/0
```

   # Run the **display current-configuration interface** *interface-type interface-number* command in any view to check the interface configuration. If the following information is displayed, LDP is enabled on the interface.

```
<HUAWEI> display current-configuration interface GigabitEthernet 1/0/0
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.2.2.1 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
 dcn
#
```

   # If private network routes are used, run the **display ip routing-table vpn-instance** *vpn-instance-name ip-address* command in any view and check outbound interface information.

```
<HUAWEI> display ip routing-table vpn-instance vpn1 10.3.2.1
```



```
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : vpn1
Summary Count : 1
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
10.4.2.0/24         Direct  0    0         D   10.5.6.5        Ethernet0/0/1
```

Run the **display mpls ldp remote-peer peer-id** *lsr-id* command in any view and check the name of a remote LDP peer.

```
<HUAWEI> display mpls ldp remote-peer peer-id 10.1.1.2

                    LDP Remote Entity Information
 ------------------------------------------------------------------------------
 Remote Peer Name  : 5to3
 Remote Peer IP    : 10.1.1.2         LDP ID       : 10.1.1.1:0
 Transport Address : 10.1.1.1          Entity Status : Active

 Configured Keepalive Hold Timer : 45 Sec
 Configured Keepalive Send Timer : ---
 Configured Hello Hold Timer     : 45 Sec
 Negotiated Hello Hold Timer     : 45 Sec
 Configured Hello Send Timer     : ---
 Configured Delay Timer         : 10 Sec
 Hello Packet sent/received      : 272/271
 Label Advertisement Mode       : Downstream Unsolicited
 Remote Peer Deletion Status     : No
 Auto-config                  : ---
 ------------------------------------------------------------------------------
```

Run the **display current-configuration configuration mpls-ldp-remote** *name* command in any view and check the configuration in the remote LDP peer view. The following information indicates that a remote adjacency is configured.

```
<HUAWEI> display current-configuration configuration mpls-ldp-remote 5to3
#
mpls ldp remote-peer 5to3
 remote-ip 10.1.1.2
#
return
```

3. If any of the following configurations exists in the interface view or remote LDP peer view, the problem may occur.
   a. For the same LDP peer, the **mpls ldp transport-address** command is run in some local interface views and remote LDP peer view, or this command is run in all local interface views and remote LDP peer view but the configured parameters differ.
   b. Different transport addresses are specified when the **mpls ldp transport-address** command is run in all local interface views of the same private LDP peer.
   c. For the same LDP peer, the **mpls ldp timer keepalive-hold** command is run in some local interface views and remote LDP peer view, or this command is run in all local interface views and remote LDP peer view but the configured parameters differ.
   d. For the same LDP peer, the **mpls ldp timer keepalive-send** command is run in some local interface views and remote LDP peer view, or this command is run in all local interface views and remote LDP peer view but the configured parameters differ.

e. For the same LDP peer, the **mpls ldp advertisement** command is run in some local interface views and remote LDP peer view, or this command is run in all local interface views and remote LDP peer view but the configured parameters differ.

f. For the same LDP peer, the **mpls ldp local-lsr-id** command is run in some local interface views and remote LDP peer view, or this command is run in all local interface views and remote LDP peer view but the configured parameters differ.

Recovery measures:

For the same LDP peer, one of the following commands is run in some local interface views and remote LDP peer view, or this command is run in all local interface views and remote LDP peer view but the configured parameters differ. In this situation, you must use the same or default parameter in the local interface views and remote LDP peer view in the following commands:

- **mpls ldp transport-address**
- **mpls ldp transport-address**
- **mpls ldp timer keepalive-hold**
- **mpls ldp timer keepalive-send**
- **mpls ldp advertisement**
- **mpls ldp local-lsr-id**

1.8.1.2 Configure LDP-IGP Synchronization on the Interface

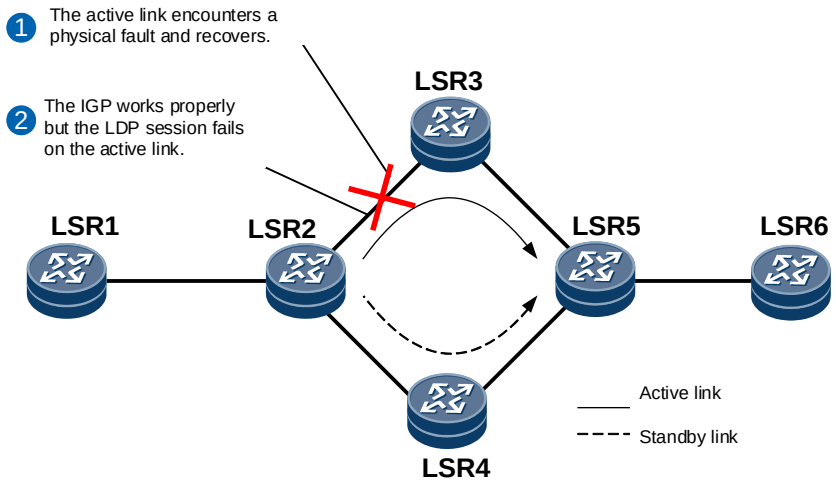
LDP is enabled on the interface, but LDP-IGP synchronization is not enabled. During LDP session flapping or link fault recovery, services carried on the LDP tunnel are compromised or interrupted.

Scenario

The LDP convergence speed depends on the IGP route convergence speed. Consequently, LDP convergence is slower than IGP convergence. Figure 1-4 shows a network with the active and standby links.

- If the active link fails, the IGP route and LSP are switched to the standby link (using LDP FRR). When the active link recovers, the IGP route switches to the active link before the LDP LSP over the active link recovers. After traffic is switched to the active IGP route, traffic is discarded on the LDP LSP that is not established.
- When the IGP route of the active link is available but the LDP session over the active link fails, this IGP route takes effect, whereas the LDP LSP over the active link is deleted. In addition, no preferred IGP route passes through the standby link, and the LSP cannot be established on the standby link. As a result, LSP traffic is lost.

Figure 1-15 Service compromised without LDP-IGP synchronization configured on an LDP interface



Configuration Requirements

In the view of an MPLS LDP-enabled interface, you must configure LDP-IGP synchronization and set the hold-max-cost timer to infinite. An IGP can be IS-IS or OSPF. You can configure the synchronization capability based on service requirements on the live network.

Misconfiguration Risks

Risk description:

Run the **display current-configuration interface** command in any view and check LDP-enabled interface information. The command output shows that LDP-IGP synchronization is not configured on an interface. If no information is displayed after you run the **display mpls lsp protocol ldp include ip-address 32** command in the user view, the LDP LSP that is to carry services fails to be established. During LDP session flapping or link fault recovery, services carried on the LDP LSP are restored slowly or keep failing to be restored. As a result, services carried on the LDP LSP are compromised or interrupted.

Identification method:

Run the **display current-configuration interface** command in any view and check the interface configuration. The problem may occur if MPLS LDP is configured in the interface view but LDP-IGP synchronization is not configured.

If the following information is displayed, MPLS LDP is configured in the interface view. In addition, synchronization between LDP and IS-IS and between LDP and OSPF is configured.

```
<HUAWEI> display current-configuration interface
#
interface GigabitEthernet1/0/0
 undo shutdown
 mtu 9192
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
```



```
isis ldp-sync
 isis timer ldp-sync hold-max-cost infinite
 ospf ldp-sync
 ospf timer ldp-sync hold-max-cost infinite
 mpls
 mpls ldp
 dcn
 negotiation auto
#
…
```

Recovery measures:

In the view of an MPLS LDP-enabled interface, configure LDP-IGP synchronization and set the hold-max-cost timer to infinite.

```
<HUAWEI> display current-configuration interface
#
interface GigabitEthernet1/0/0
 undo shutdown
 mtu 9192
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
isis ldp-sync
 isis timer ldp-sync hold-max-cost infinite
 ospf ldp-sync
 ospf timer ldp-sync hold-max-cost infinite
 mpls
 mpls ldp
…
```

1.8.2 MPLS TE Configuration Instructions

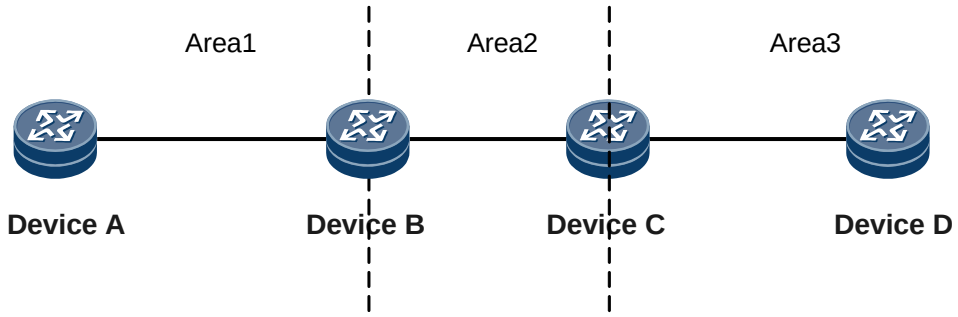
1.1.1.1 Configure Explicit Paths to Establish TE Tunnels Across IGP Areas

A TE tunnel that traverses through multiple IGP areas fails to be established if the explicit path that contains the IP address of a cross-IGP-area node is not configured for the tunnel and CSPF is configured on all devices through which the tunnel passes.

Scenario

A TE tunnel is established across IGP areas.

Figure 1-16 Inter-IGP-area tunnel establishment failure



As shown in Figure 1-5, a TE tunnel is established from router A to router D. The outbound interface of router A and the inbound interface of router B belong to IGP area 1. The outbound interface of router B and the inbound interface of router C belong to IGP area 2. The outbound interface of router C and the inbound interface of router D belong to IGP area 3. Router B and router C are inter-area nodes.

Configuration Requirements

When a TE tunnel traverses through multiple IGP areas, the explicit path that contains the IP address of the cross-IGP-area node must be configured for the tunnel, and CSPF must be enabled on both the ingress and cross-IGP-area node.

Misconfiguration Risks

Risk description:

A TE tunnel that traverses through multiple IGP areas fails to be established if the explicit path that contains the IP address of a cross-IGP-area node is not configured for the tunnel and CSPF is configured on all devices through which the tunnel passes.

Identification method:

1 Run the **display current-configuration configuration mpls** command in the user view and check the global MPLS configurations.

The following information shows that MPLS TE and MPLS TE CSPF are configured.

```
<HUAWEI> display current-configuration configuration mpls
#
mpls lsr-id 10.1.1.1
#
mpls
 mpls te
 mpls rsvp-te
 mpls te cspf
#
return
```

2. Run the **display current-configuration interface** *interface-type interface-number* command in the user view to check the tunnel configuration and obtain the destination address and explicit path of the tunnel.

The command output shows that the destination address of the tunnel is **10.4.4.4** and the explicit path is **huawei**.

```
<HUAWEI> display current-configuration interface Tunnel 0/0/1
#
interface Tunnel0/0/1
 tunnel-protocol mpls te
 destination 10.4.4.4
 mpls te record-route
 mpls te backup hot-standby
 mpls te tunnel-id 1
 mpls te path explicit-path huawei
#
return
```


3. Run the **display mpls te cspf tedb all** command in the user view and check CSPF TEDB information. If there is no destination IP address of the tunnel, an inter-IGP-area scenario is the case.

   The following command output shows that the TEDB does not contain an LSP destined for **10.4.4.4**, which indicates an inter-IGP-area scenario.

```
<HUAWEI> display mpls te cspf tedb all
Maximum Nodes Supported: 2000   Current Total Node Number: 4
Maximum Links Supported: 8000   Current Total Link Number: 6
Maximum SRLGs supported: 10000  Current Total SRLG Number: 0
Id    Router-Id       IGP     Process-Id    Area          Link-Count
1     10.1.1.1         ISIS    1           Level-1        2
2     10.2.2.2         ISIS    1           Level-1        1
3     10.1.1.1         ISIS    1           Level-2        2
4     10.2.2.2         ISIS    1           Level-2        1
```

4. Check whether the explicit path of the tunnel is correct.
   - If the explicit path is not configured, you must configure the explicit path that contains the IP address of the cross-IGP-area node.
   - If an explicit path is configured, run the **display current-configuration configuration explicit-path** *explicit-name* command in the user view and check whether the explicit path contains the IP address of the inter-IGP area node.

```
<HUAWEI> display current-configuration configuration explicit-path test
#
explicit-path test
 next hop 192.168.1.2 include loose
#
```

Recovery measures:

When a TE tunnel traverses multiple IGP areas, configure the explicit path that contains the IP address of the cross-IGP-area node for the tunnel, and enable CSPF on both the ingress and cross-IGP-area node.

1.8.2.2 Before RSVP-TE GR Is Used, Configure the RSVP-TE Hello Function on an RSVP-TE Interface

If you run the **mpls rsvp-te hello support-peer-gr** or **mpls rsvp-te hello full-gr** command in the MPLS view when deploying RSVP-TE GR, you must run the **mpls rsvp-te hello** command on the RSVP-TE-enabled interface.

Scenario

RSVP-TE GR is configured. For details about the scenario, see Configuring RSVP GR in the related configuration guide.

Configuration Requirements

When deploying RSVP-TE GR, you must configure RSVP-TE Hello on an RSVP-TE interface.

Misconfiguration Risks

Risk description:

If the RSVP-TE Hello function is not configured on the RSVP-TE interface, RSVP-TE GR fails. If an RSVP node performs a primary/backup CR-LSP switchover, the RSVP neighbor relationship between this node and its neighbor is torn down due to a signaling protocol timeout. As a result, the CR-LSP is deleted, and services carried on the CR-LSP are interrupted.

Identification method:

1. Run the **display current-configuration configuration mpls** command in the user view and check whether the **mpls rsvp-te hello support-peer-gr** or **mpls rsvp-te hello full-gr** command exists in the global MPLS configurations. The following information indicates that GR is deployed.

```
<HUAWEI> display current-configuration configuration mpls

#
mpls lsr-id 10.1.1.1
#
mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te hello
 mpls rsvp-te hello support-peer-gr
 mpls te cspf
#
return
```

2. Run the **display current-configuration interface** command in the user view and check whether the **mpls rsvp-te hello** command is configured on the interface. If the **mpls rsvp-te hello** command is not run on the interface, the problem occurs.

```
<HUAWEI> display current-configuration interface
#
interface Ethernet3/0/0
 undo shutdown
 ip address 192.168.21.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls rsvp-te hello
#
```

Recovery measures:

Run the **mpls rsvp-te hello** command in the view of Ethernet 3/0/0 to enable the Hello mechanism on the interface.

1.8.2.3 Configure Explicit Paths to Prevent Unexpected CSPF Path Calculation Results

When multiple IGP processes with MPLS TE enabled are deployed on a device, CSPF cannot compute the optimal path among multiple IGP processes. The optimal path computed in an

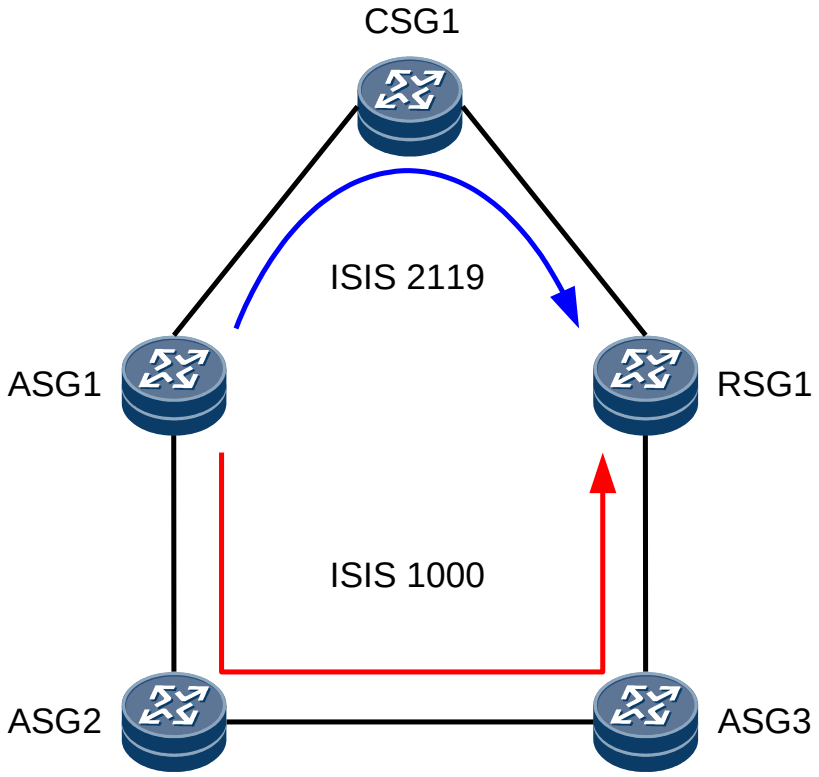
individual process may differ from the expected path. Consequently, services carried on the TE tunnel established over the computed path may be congested with traffic or interrupted.

Scenario

As shown in Figure 1-17, a TE tunnel is deployed on a device, and multiple paths through which the tunnel may traverse belong to different IGP processes.

IS-IS is used as an example. A TE tunnel is established from ASG1 to RSG1. Multiple IS-IS processes (IS-IS 1000 and IS-IS 2119) exist between the ingress and egress. If no fault occurs, the red tunnel path is displayed in Figure 1-17. If route flapping occurs on the access ring in the IS-IS process of ID 2119, the tunnel path bypasses the CSG after the TE re-optimization time elapses, as shown in the blue line in Figure 1-17.

Figure 1-17 CSPF computation results different from expected ones in multi-IGP-process or multi-IGP-area scenarios



Configuration Requirements

When MPLS TE is enabled for multiple IGP processes, the processes instruct CSPF to update TEDB information in sequence. When CSPF calculates paths for TE tunnels, information about the IGP process that is last updated to the TEDB takes effect. The optimal path cannot be computed by comparing the IGP costs of different IGP processes. The optimal path computed in a single process may differ from the expected one.

During the configuration, select either of the following two schemes:

1 Recommended solution: Configure an explicit path in the system view and reference it in the TE tunnel interface view. An explicit path named **pri1** is used as an example.

Run the **explicit-path pri1** command in the system view to configure an explicit path.

```
<HUAWEI> system-view
[HUAWEI] explicit-path pri1
```

Run the **mpls te path explicit-path pri1** command in the TE tunnel interface view to specify an explicit path.

```
[HUAWEI] interface Tunnel 0/0/1
[HUAWEI-Tunnel0/0/1] tunnel-protocol mpls te
[HUAWEI-Tunnel1/0/0] mpls te path explicit-path pri1
[HUAWEI-Tunnel1/0/0] mpls te commit
```

NOTE

In a cross-IGP-area scenario on the live network, an explicit path must contain the inter-area devices and CSPF must be enabled on such devices.

An explicit path must also be configured for an HSB LSP. Otherwise, the problem also occurs in the same scenario.

2. Alternative solution: Run the **mpls te cspf preferred-igp** command in the MPLS view to enable CSPF to preferentially select a specified IGP process during path computation.

   # If IS-IS processes are used, run the **mpls te cspf preferred-igp isis 1** command in the MPLS view to configure a preferred IS-IS process.

   ```
   <HUAWEI> system-view
   [HUAWEI] mpls
   [HUAWEI-mpls] mpls te cspf preferred-igp isis 1
   ```

   # If OSPF processes are used, run the **mpls te cspf preferred-igp ospf 1 area 0.0.0.0** command in the MPLS view to configure a preferred OSPF process and area. The **area** *area-id* parameter is optional.

   ```
   <HUAWEI> system-view
   [HUAWEI] mpls
   [HUAWEI-mpls] mpls te cspf preferred-igp ospf 1 area 0.0.0.0
   ```

   NOTE

   It is recommended that this solution be used as an alternative solution. Even if the preferred IGP process is configured, CSPF fails to use the preferred IGP process to compute paths (for example, link flapping occurs temporarily). In this case, another process is selected to compute paths. If other processes are used to compute paths, LSPs are created. To switch back traffic to the preferred IGP process, wait for TE re-optimization to trigger CSPF re-computation. Therefore, this solution does not prevent this problem for good.

   In addition, only a single preferred process can be configured. This solution is not applicable if each TE tunnel requires a specific preferred IGP process (for example, RSGs belong to multiple aggregation rings and a specific IGP process is created for each aggregation ring).

Misconfiguration Risks

Risk description:

TE tunnels and IGP multi-processes are deployed on the ingress and egress. TE LSPs on the ingress and egress are automatically computed to pass through IGP paths. Explicit paths or other constraints are not configured. As a result, the paths traversed through by the TE tunnels are different from the expected ones, and services are congested or interrupted.

Identification method:

1 Check whether MPLS TE, RSVP-TE, and CSPF are enabled.

If MPLS TE, RSVP-TE, and CSPF are enabled, the problem described in this case may occur. Further check is required. If any of the preceding functions is not enabled, the problem does not occur.


```
<HUAWEI> display current-configuration configuration mpls
#
mpls lsr-id 10.2.2.2
mpls
 mpls te
 mpls rsvp-te
 mpls te cspf
#
return
```

3. Check whether multiple IS-IS or OSPF processes exist.

   # Run the **display current-configuration configuration isis** or **display current-configuration configuration ospf** command in the user view. If multiple IS-IS or OSPF processes exist, the problem may occur. In this case, you must perform further check.

```
<HUAWEI> display current-configuration configuration isis
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 10.0000.0002.0001.00
 traffic-eng level-2
#
isis 2
 is-level level-2
 cost-style wide
 network-entity 10.0000.0002.0002.00
 traffic-eng level-2
…
#
<HUAWEI> display current-configuration configuration ospf
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 10.1.1.2 0.0.0.0
  network 10.2.2.1 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.20.20.20 0.0.0.0
  mpls-te enable
#
ospf 2
 area 0.0.0.0
  network 10.1.10.0 0.0.0.255
  network 10.1.11.0 0.0.0.255
…
```

4. Check whether TE is enabled for IS-IS or OSPF.

   # Use the same command in the same view as that in Step 2. If TE is enabled for more than one IS-IS or OSPF process, the problem may occur. In this case, go to Step 5. If TE is enabled only in a single OSPF process, go to Step 4. If TE is enabled only in a single IS-IS process, the problem does not occur.

```
<HUAWEI> display current-configuration configuration isis
#
isis 1
 is-level level-2
```



```
 cost-style wide
 network-entity 10.0000.0002.0001.00
 traffic-eng level-2
#
<HUAWEI> display current-configuration configuration ospf
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 10.1.1.2 0.0.0.0
  network 10.2.2.1 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.20.20.20 0.0.0.0
  mpls-te enable
```

5. Check whether multiple areas are configured for OSPF.

   # Run the **display current-configuration configuration ospf** command in the user view. If multiple OSPF areas exist and MPLS TE is enabled in each area, the problem may occur. In this case, you must perform further check.

```
<HUAWEI> display current-configuration configuration ospf
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 10.1.1.2 0.0.0.0
  mpls-te enable
area 0.0.0.9
 network 10.1.1.9 0.0.0.0
 mpls-te enable
```

6. Query the actual path of the tunnel.

   Check whether the path through which the tunnel traverses is consistent with the planned path. If they are inconsistent, the problem described in this case occurs.

   - Run the **display current-configuration interface Tunnel 0/0/1** command in the user view and check whether a route is configured. The tunnel interface **Tunnel 0/0/1** is used as an example.

```
<HUAWEI> display current-configuration interface Tunnel 0/0/1
#
interface Tunnel0/0/1
 tunnel-protocol mpls te
 destination 10.4.4.4
 mpls te record-route label
 mpls te backup hot-standby
 mpls te tunnel-id 111
#
Return
```

   - If the **mpls te record-route label** command is run, run the **display mpls te tunnel path Tunnel0/0/1** command in the user view and check information about the path through which the tunnel passes.

```
<HUAWEI> display mpls te tunnel path Tunnel0/0/1
 Tunnel Interface Name : Tunnel0/0/1
 Lsp ID : 10.3.3.3 :100 :3
 Hop Information
  Hop 0   10.3.3.3
```



```
  Hop 1   10.1.1.1
  Hop 2   10.1.1.2
  Hop 3   10.2.2.2
```

- If the **mpls te record-route label** command is not run, run the **tracert lsp te Tunnel 0/0/1** command in the user view and check information about the path through which the tunnel traverses.

```
<HUAWEI> tracert lsp te Tunnel 0/0/1
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel0/0/1, press
CTRL C to break.
  TTL   Replier          Time    Type     Downstream
  0                           Ingress   10.1.2.1/[3 ]
  1     10.3.3.3          32 ms   Egress
```

Recovery measures:

Recommended solution: Configure an explicit path in the system view and reference it in the TE tunnel interface view.

Alternative solution: Run the **mpls te cspf preferred-igp** command in the MPLS view to enable CSPF to preferentially select a specified IGP process during path computation.

1.8.2.4 Configure a Remote LDP Session After Route Advertisement Is Configured for a TE Tunnel

In an LDP over TE scenario, after the **mpls te igp advertise** or **mpls te igp advertise shortcut** command is run in the TE tunnel interface view to enable route advertisement, a remote LDP session must be configured, with the remote IP address set to the destination IP address of the tunnel.

Scenario

In an LDP over TE scenario, a TE tunnel interface exists and the **mpls te igp advertise** or **mpls te igp advertise shortcut** command is run on the TE tunnel interface.

Configuration Requirements

In an LDP over TE scenario, after the **mpls te igp advertise** or **mpls te igp advertise shortcut** command is run in the TE tunnel interface view, a remote LDP session with the remote IP address set to the destination IP address must be configured.

Misconfiguration Risks

Risk description:

If no remote LDP session is configured, no LDP LSP can be established. As a result, services are interrupted.

Identification method:

1. Run the **display current-configuration interface** *interface-name* command in the user view, check whether the **mpls te igp advertise** or **mpls te igp advertise shortcut** command is run for the tunnel, and record the destination address.

```
<HUAWEI> display current-configuration interface Tunnel0/0/1
#
interface Tunnel0/0/1
 ip address unnumbered interface LoopBack0
```



```
tunnel-protocol mpls te
destination 10.1.1.1
mpls te tunnel-id 2000
mpls te igp advertise
mpls te commit
```

2. Run the **display current-configuration configuration mpls-ldp-remote** command in the user view. If no remote LDP peer with the remote IP address set to the destination IP address of the tunnel exists, the problem described in this case occurs.

```
<HUAWEI> display current-configuration configuration mpls-ldp-remote
#
mpls ldp remote-peer test
remote-ip 10.10.10.1
#
return
```

Recovery measures:

After the **mpls te igp advertise** or **mpls te igp advertise shortcut** command is run in the TE tunnel interface view, configure a remote LDP session with the remote IP address set to the destination IP address of the tunnel.

1.8.2.5 Configure a Hello Session Between the PLR and MP of a Bypass Tunnel in a TE FRR Scenario

On a network where TE FRR is deployed, to protect traffic on the primary tunnel if both FRR and RSVP-TE GR are faulty, a Hello session must be established between the point of local repair (PLR) and merge point (MP) of a bypass tunnel.

Scenario

TE FRR is deployed on a network.

Configuration Requirements

On a network where TE FRR is deployed, a Hello session must be created between the PLR and MP of a bypass tunnel, and the **mpls rsvp-te hello nodeid-session** *ip-address* command must be run in the MPLS view.

Misconfiguration Risks

Risk description:

If the Hello function is not configured, the enhanced RSVP GR function is not supported, and services are interrupted.

Identification method:

1. Run the **display current-configuration interface** *interface-name* command in the user view and check whether the **mpls te fast-reroute** command is run for the tunnel.

```
<HUAWEI> display current-configuration interface Tunnel0/0/1
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
```



```
destination 10.1.2.9
mpls te tunnel-id 2000
mpls te fast-reroute
mpls te commit
```

2. Run the **display current-configuration configuration mpls** command in the user view. If GR is configured but the **mpls rsvp-te hello nodeid-session** *ip-address* command is not run, the problem described in this case occurs.

```
<HUAWEI> display current-configuration configuration mpls
#
 mpls lsr-id 10.2.2.2
 mpls
  mpls te
  mpls rsvp-te
  mpls rsvp-te Hello
  mpls rsvp-te Hello full-gr
  mpls rsvp-te Hello nodeid-session ip-address
  mpls te cspf
```

Recovery measures:

On the PLR and MP, run the **mpls rsvp-te Hello nodeid-session** *ip-address* command in the MPLS view. (On the PLR, *ip-address* is the MP's LSR ID. On the MP, *ip-address* is the PLR's LSR ID.)

1.9 VPN

1.9.1 BGP/MPLS IP VPN Configuration Instructions

1.1.1.1 Activate a License for the L3VPN Service Configured on a Type-B Board

A license must be activated for an L3VPN service before the service is transmitted on a type-B board. If the license is not activated, the L3VPN service is interrupted.

Scenario

NOTE

Type-B boards refer to the boards whose names contain the -B or Unit B characters.

To view a board name, check the **Description** field in the **display elabel** command output.

1. Scenario 1: A non-type-B board used for a device to carry an L3VPN service is to be replaced with a type-B board.
2. Scenario 2: A type-B board is used for a device to carry an L3VPN service, but the license for the L3VPN service expires.
3. Scenario 3: A device uses a type-B board for the first time to carry an L3VPN service.

Configuration Requirements

In scenario 1, the following procedure must be performed:

1 Apply for a GTL license according to the model of the type-B board. For details about the application, contact Huawei technical support.

4. Upload the GTL license file to the root directory of the CF card on the master main control board of the device. For details, see "Example for Operating Files" in the product manual. If the slave main control board exists, run the **copy** *source-filename* **slave#cfcard:/** *destination-filename* command to copy the GTL license file to the root directory of the CF card on the slave main control board.
5. Run the **license active** *file-name* command to activate the GTL license.
6. Replace the non-type-B board with the type-B board. For details, see **Part Replacement** -> **Replacing Boards** -> **Replacing a Service Processing Board**.
7. Power on the type-B board and run the **service-enhance slot** *slot-id* command to load the GTL license file to the type-B board so that the board can support L3VPN services.

In scenario 2, the following procedure must be performed:

1 Apply for a GTL license according to the model of the type-B board. For details about the application, contact Huawei technical support.

8. Upload the GTL license file to the root directory of the CF card on the master main control board of the device. For details, see "Example for Operating Files" in the product manual. If the slave main control board exists, run the **copy** *source-filename* **slave#cfcard:/** *destination-filename* command to copy the GTL license file to the root directory of the CF card on the slave main control board.
9. Run the **license active** *file-name* command to activate the GTL license.

In scenario 3, the following procedure must be performed:

1 Install the type-B board and power on the device. For details, see **Installation** -> **Installing Boards and Subcards**.

10. Apply for a GTL license according to the model of the type-B board. For details about the application, contact Huawei technical support.
11. Upload the GTL license file to the root directory of the CF card on the master main control board of the device. For details, see "Example for Operating Files" in the product manual. If the slave main control board exists, run the **copy** *source-filename* **slave#cfcard:/** *destination-filename* command to copy the GTL license file to the root directory of the CF card on the slave main control board.
12. Run the **license active** *file-name* command to activate the GTL license.
13. Run the **service-enhance slot** *slot-id* command to load the GTL license file to the type-B board so that the board can support L3VPN services.

Misconfiguration Risks

Risk description:

By default, a type-B board does not support L3VPN. A GTL license must be applied for and activated, and L3VPN must be enabled before the type-B board can transmit an L3VPN service. If the GTL license is missing, is not activated, or has expired, the L3VPN service is interrupted on the type-B board.

Identification method:

- **In scenario 1:**

  Check whether the L3VPN service exists on the non-type-B board. Run the **display fib** *slot-id* **statistics all** command to check whether VPN forwarding-related statistics exist on the non-type-B board. In the following example command output, the **IPv4 FIB VPN-instance 1 Route Prefix Count**, **IPv4 FIB VPN-instance 2 Route Prefix Count**, **IPv4 FIB VPN-instance dsc Route Prefix Count** all have counts, indicating that the

board in slot 4 is carrying an L3VPN service. Apply for a GTL license before the board replacement.

```
<HUAWEI> display fib 4 statistics all
IPv4 FIB Route Prefix Capacity : 3379199
IPv4 FIB Total Route Prefix Count : 40; Entry Count : 41

IPv4 FIB Public Route Prefix Count : 34; Entry Count : 35
IPv4 FIB VPN-instance 1 Route Prefix Count : 1; Entry Count : 1
IPv4 FIB VPN-instance 2 Route Prefix Count : 1; Entry Count : 1
IPv4 FIB VPN-instance dsc Route Prefix Count : 4; Entry Count : 4
```

- **In scenario 2:**

  Run the **display license** command to check the validity of the GTL license. In the following example command output, the value of the **Expired date** field indicates that the license has expired. In this case, apply for a new GTL license.

```
<HUAWEI> display license
Active license : cfcard:/licortf201476-f2cffd7e56_me60.dat
License state : Normal
Revoke ticket : No ticket

RD of Huawei Technologies Co., Ltd.

Product name : ME60
Product version : V600R008
License Serial No : LIC2014081100D550
Creator : Huawei Technologies Co., Ltd.
Created Time : 2012-08-11 14:02:06
Feature name : MEFEA
Authorize type : COMM
Expired date : 2017-08-11
Trial days : --
Feature name : MEFEB
Authorize type : COMM
Expired date : 2017-08-11
Trial days : --

Item name Item type Value Description
-------------------------------------------------------------
LME0NGMVPN Function YES Multicast NG MVPN
LME0HAGF01 Function YES Cross-chassis HAG
LME0FWF01 Function YES Firewall for SSU
LME0P8200G00 Function YES SWCAP
LME0BRAS01 Function YES BRAS Function(4k subscribers)
LME0MDI00 Function YES DIST MQE License
LME0VPDN01 Function YES LNS&LTS Function
LME0RDPXY00 Function YES Radius-proxy Function
LME0LIF01 Function YES Lawful Interception
LME0EPT00 Function YES RFC2544 Function
LME0FPM00 Function YES IP FPM Function
LME0SSGF01 Function YES DSG Function
LME0WIFI00 Function YES ME60 Wifi Gateway Enhance Function License
LME0REMMIR00 Function YES Remote Mirroring License
LME0CONN01 Resource 256 Concurrent Users(1k)
LME0SMVP00 Resource 32 EnhanceLicense MVPN
LME0STUN00 Resource 32 TUNNEL
```



```
LME0SNAT00 Resource 32 NAT for SPU C
LME0SNET00 Resource 32 ENHANCE_NS
LME0VIDE00 Resource 32 MQE License
LME0IPSEC00 Resource 32 IPSEC License
LME0NATDS00 Resource 256 2M NAT Session
LME0L2NATDS00 Resource 32 L2NAT license
LME0DSLITEDS00 Resource 32 DS-lite license
LME04020G00 Resource 32 20G NAT BandWidth
LME0L2NAT01 Resource 32 L2NAT License for VSUF
LME0DSLITE01 Resource 32 DS-Lite License for VSUF
LME0PCP00 Resource 32 PCP License for VSUF
LME0NAT6401 Resource 32 NAT64 License for VSUF
LME0TUNL00 Resource 224 GTL license for Hybrid Access Tunnel
LME0SGTN00 Resource 16 ME60 SoftGRE 1k Tunnel License

Item name (View)Resource License Command-line
------------------------------------------------------------
LME0IPSEC00 (License)active ipsec slot slot-id
LME0NATDS00 (License)active nat session-table size
LME0L2NATDS00 (License)active l2nat slot slot-id
LME0DSLITEDS00 (License)active ds-lite slot slot-id
LME04020G00 (License)active nat bandwidth-enhance slot slot-id
LME0L2NAT01 (License)active l2nat vsuf slot slot-id
LME0DSLITE01 (License)active ds-lite vsuf slot slot-id
LME0PCP00 (License)active pcp vsuf slot slot-id
LME0NAT6401 (License)active nat64 vsuf slot slot-id

Master board license state: Normal.
```

- **In scenario 3:**

  None

Recovery measures:

Perform specific steps according to different scenarios described in "Configuration Requirements".

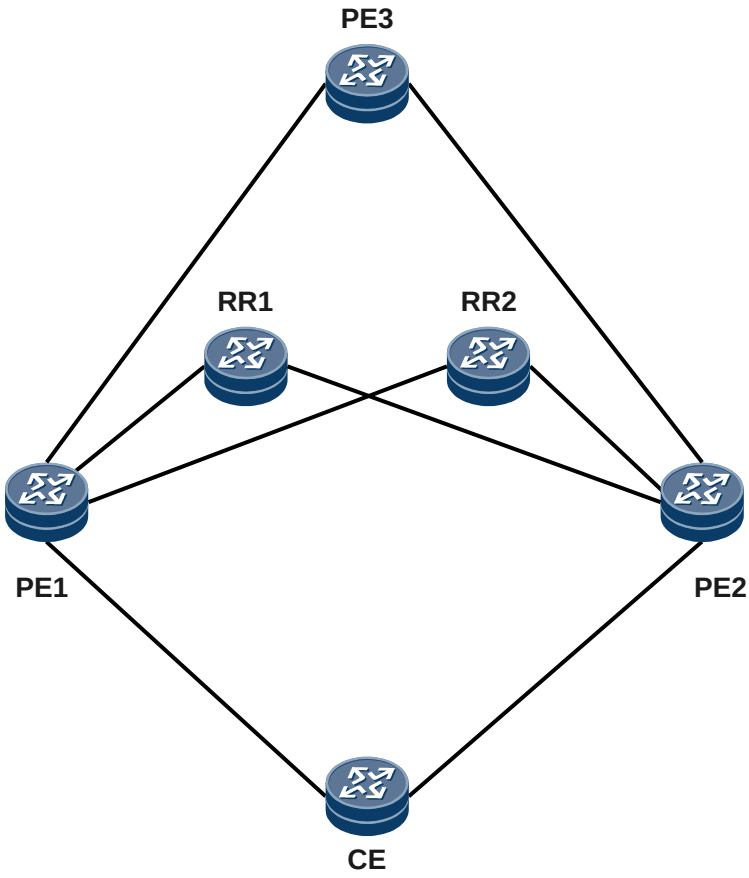
1.9.1.2 Configure Different RDs for the Same VPN Instance on Two Dual-Homing PEs

In a scenario where a CE is dual-homed to PEs and the same VPN instance on each PE is configured with the same RD, after the PEs send BGP routes to an RR, a remote PE receives only one BGP route reflected by the RR, causing VPN FRR on the remote PE to fail.

Scenario

On the network shown in Figure 1-18, a CE is dual-homed to PE1 and PE2. The same VPN instance on each PE is configured with the same RD, causing VPN FRR to fail on PE3.

Figure 1-18 VPN FRR failure on a CE dual-homing network



Configuration Requirements

Different RDs must be configured for the same VPN instance on the dual-homing PEs.

Misconfiguration Risks

Risk description:

If the master PE fails or the tunnel between the master PE and PE3 goes faulty, PE3 fails to generate VPN FRR entries, which cannot trigger a VPN FRR switchover. As a result, packet loss lasts several seconds.

Identification method:

1 Check the configurations on PE1 and PE2 to find the same VPN instance with the same RD.

2. In any view of PE3, run the **display ip routing-table vpn-instance** *vpn-instance-name ip-address* **verbose** command to check the VPN routing table information. If no backup next hop, backup tunnel, or VPN label is displayed, no VPN FRR entry is generated on PE3.

```
<HUAWEI> display ip routing-table vpn-instance vpn1 10.1.1.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
```



```
Routing Table : vpn1
Summary Count : 1

Destination: 10.3.1.0/24
    Protocol: BGP          Process ID: 0
  Preference: 255               Cost: 0
     NextHop: 10.2.2.2       Neighbour: 10.2.2.2
       State: Active Adv GotQ      Age: 00h15m06s
         Tag: 0             Priority: low
       Label: 15361           QoSInfo: 0x0
  IndirectID: 0x13
RelayNextHop: 0.0.0.0        Interface: Pos2/0/0
    TunnelID: 0x6002002          Flags: RD
```

Recovery measures:

Configure different RDs for the same VPN instance on the dual-homing PEs.

1.9.1.3 Associate a New BFD Session With an Interface and Bind the Original Static Route to the New BFD Session After Unbinding the Interface from a VPN Instance

When an interface is unbound from a VPN instance, the BFD session associated with the interface is deleted accordingly. As a result, the status of a static route bound to the BFD session may change, causing services to deteriorate.

Scenario

On the network shown in Figure 1-19:

1. A VPN instance is bound to GE 1/0/0 using the **ip binding vpn-instance** *vpn-instance-name* command.
2. A static BFD session is bound to the interface in step 1.
3. A static route is associated with the static BFD session in step 2.

When the **ip binding vpn-instance** *vpn-instance-name* command configuration is deleted from the interface in step 1, configuration of the static BFD session is deleted accordingly. In this case, the association between the BFD session and the static route is removed, causing services to deteriorate in some scenarios.

Figure 1-19 Deletion of an associated BFD session

A static BFD session is established between Device 1 and Device 2, and the BFD session is bound to the interconnected interfaces GE 1/0/0 of the devices. Perform the following steps to check the problem consequence.

1 Run the following commands to view the configurations of GE 1/0/0 and the BFD session on Device 1.


```
[Huawei] display current-configuration interface GigabitEthernet1/0/0
#
interface GigabitEthernet1/0/0
 ip binding vpn-instance vpn1   //Bind a VPN instance to GE 1/0/0.
 ip address 10.0.0.1 255.255.255.0
#
return
[Huawei] display current-configuration configuration bfd-session
#
bfd bfd1 bind peer-ip 10.0.0.2 vpn-instance vpn1 interface GigabitEthernet1/0/0
 discriminator local 1
 discriminator remote 2
 commit   //Bind a BFD session named BFD1 to the interface.
```

4. Check the BFD session status on Device 1.

```
<HUAWEI> display bfd session all
--------------------------------------------------------------------------------
-
Local Remote    PeerIpAddr     State    Type       InterfaceName
--------------------------------------------------------------------------------
-
1    2        10.0.0.2       Up       S IP IF    GigabitEthernet1/0/0
--------------------------------------------------------------------------------
-
    Total UP/DOWN Session Number : 1/0
```

5. Check the configuration and status of the static route on Device 1.

```
[Huawei] display current-configuration  | include ip route
ip route-static 10.0.0.0 255.255.255.0 10.0.0.3 track bfd-session bfd1
//Associate the static route with the BFD session named BFD1.
```

The static route is active.

```
[Huawei] display ip routing-table 10.0.0.1
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.0.0/24  Static  60   0           RD  10.0.0.3        GigabitEthernet1/0/0
```

6. After the BFD session named **BFD1** goes down, the static route on Device 1 is withdrawn.

```
[Huawei] display bfd session all
--------------------------------------------------------------------------------
-
Local Remote    PeerIpAddr     State    Type       InterfaceName
--------------------------------------------------------------------------------
-
1    2        10.0.0.2       Down     S IP IF    GigabitEthernet1/0/0    //The
BFD session is Down.
--------------------------------------------------------------------------------
[Huawei] display ip routing-table 10.0.0.1  //The static route has been withdrawn.
```

7. Delete the **ip binding vpn-instance** *vpn-instance-name* command configuration on GE 1/0/0.


```
[Huawei-GigabitEthernet1/0/0] undo ip binding vpn-instance vpn1  //Unbind the VPN instance from the interface.
[Huawei] display current-configuration | include ip route
ip route-static 10.0.0.0 255.255.255.0 10.0.0.3  //Association between the static route and the BFD session has been deleted accordingly.
[Huawei] display ip routing-table 10.0.0.1      //The route becomes active again.
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.0.0/24  Static  60   0           RD   10.0.0.3       GigabitEthernet1/0/0
```

Configuration Requirements

When an interface is unbound from a VPN instance:

1 If a BFD session has been associated with the interface, a new static BFD session must be created and associated with the interface.

```
[Huawei]bfd bfd1 bind peer-ip 10.0.0.2 interface GigabitEthernet1/0/0
 discriminator local 1
 discriminator remote 2
 commit
```

8. If a static route has been bound to the BFD session, the static route must be bound to the new BFD session.

```
ip route-static 10.0.0.0 255.255.255.0 10.0.0.3 track bfd-session bfd1
```

Misconfiguration Risks

Risk description:

When an interface is unbound from a VPN instance, the BFD session associated with the interface is deleted accordingly, which in turn removes the association between a static route and the BFD session. As a result, the static route may become active again and recurse to an incorrect next hop, causing services to deteriorate.

Identification method:

1 Before unbinding the interface from the VPN instance, run the **display ip routing-table protocol static** command in any view and record details about the active static route.

```
<HUAWEI> display ip routing-table  protocol static
_public_ Routing Table : Static
```

9. After unbinding the interface from the VPN instance, run the **display ip routing-table protocol static** command in any view and record details about the active static route.

```
<HUAWEI> display ip routing-table protocol static
_public_ Routing Table : Static
       Destinations : 1       Routes : 1       Configured Routes : 1

Static routing table status : <Active>
       Destinations : 1       Routes : 1

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
```



```
     10.0.0.0/24  Static  60   0           D   10.0.0.2        Ethernet0/1/0

Static routing table status : <Inactive>
       Destinations : 0       Routes : 0
```

10. Compare the static route status before and after the interface is unbound from the VPN instance. If a new static route becomes active due to the deletion of its associated BFD session, the risk exists.

Recovery measures:

Associate a new BFD session with an interface and bind the original static route to the new BFD session after unbinding the interface from a VPN instance.

1.10 Security

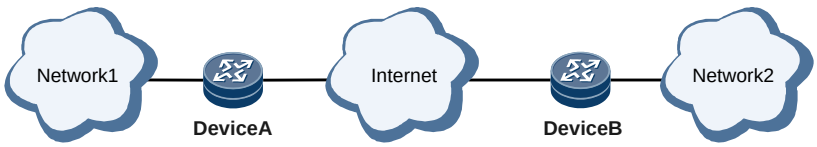
1.10.1 IPsec Configuration Instructions

1.10.1.1 In IPsec Service Scenarios, Configure IKE DPD to Ensure the Consistent Peer Status on Both Ends of an IPsec Tunnel

Dead peer detection (DPD) uses IPsec traffic to minimize the number of packets sent to monitor the peer status. The DPD mechanism does not periodically send packets. This mechanism is an alternative to the IKE keepalive mechanism. When provisioning IPsec services, you must configure IKE DPD so that both ends of an IPsec tunnel can monitor the peer status to ensure the consistent peer status.

Scenario

As shown in the following figure, an IPsec tunnel is established between device A and device B to traverse through the Internet. Network 1 and network 2 communicate with each other through this tunnel.



Configuration Requirements

The **ike dpd** command must be run to configure the DPD function.

Misconfiguration Risks

Risk description:

When the status on two ends of an IPsec tunnel becomes inconsistent, the IPsec tunnel cannot be deleted and reestablished immediately. As a result, a black hole occurs, and IPsec packets cannot be forwarded.

Identification method:

Run the **display current-configuration | include ike dpd** command and check whether **ike dpd** is contained in the command output. If this string is not displayed, IKE DPD is not configured.

```
[HUAWEI] display current-configuration | include ike dpd
 ike dpd 30
```

Recovery measures:

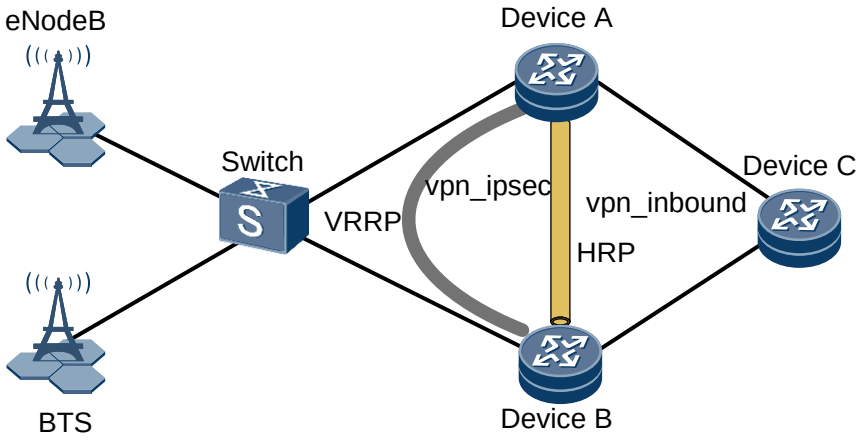
Run the **ike dpd** command to configure the DPD function.

1.10.1.2 In an IPsec Dual-Device Hot Backup Scenario, Set an MTU Value to Be Greater Than or Equal to 2000 Bytes on Each of Interconnected Interfaces of the Master and Slave IPsec Devices

Scenario

In an IPsec dual-device hot backup scenario shown in the following figure, the two IPsec devices are connected through directly connected interfaces and have HRP configured.

A security policy group is applied to the IPsec tunnel and an IPsec instance is bound to the IPsec tunnel using the **ipsec policy** *policy-name* **instance** *instance-id* command in the IPsec tunnel view. An IPsec proposal uses AH and ESP to transmit data. These two security protocols are specified using the **transform ah-esp** command run in the IPsec proposal view. With this command run, both ESP and AH are used in sequence to protect packets.



Configuration Requirements

The MTU value of the local interface that backs up data (configured using the **hrp track interface** *interface-type interface-number* command) must be greater than or equal to 2000 bytes. Perform either of the following operations based on the type of the local interface:

- If a local GE interface is used, run the **mtu** *mtu* command in the GE interface view to set an interface MTU value.
- If a local Eth-Trunk interface is used, run the **mtu** *mtu* command in the Eth-Trunk interface view to set an interface MTU value.

Misconfiguration Risks

Risk description:

In the IPsec dual-device hot backup scenario, if the MTU value on the local interface that backs up data is less than 2000 bytes, IPsec SA information fails to be backed up and services are interrupted after a master/slave device switchover is performed.

Identification method:

1. Run the **display ipsec proposal** command in the user view and check whether the **transform** field value is **ah-esp-new**. If **ah-esp-new** is displayed, both ESP and AH are used as security protocols in sequence to protect packets.

```
<HUAWEI> display ipsec proposal

  IPsec proposal name: 1
    encapsulation mode: tunnel
    transform: ah-esp-new
    AH protocol: authentication md5-hmac-96
    ESP protocol: not use authentication, encryption des
```

2. Check the interface that backs up data. Run the **display current-configuration configuration ipsec-instance** command in the user view and check the local interface of the backup link.

```
#
ipsec instance 1
 hrp peer 10.30.40.2
 hrp track interface GigabitEthernet1/0/1
 hrp vrrp vrid 1 interface GigabitEthernet1/0/1.1
 bind slot 2 backup-id 1
```

3. Run the **display interface gigabitethernet** *interface-number* command in the user view and check the MTU of the local interface. GE 1/0/1 is used as an example.

```
<HUAWEI> display interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1 current state : DOWN
Line protocol current state : DOWN
Link quality grade : --
Description:HUAWEI, GigabitEthernet1/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT ETHNT 2, Hardware address is 00e0-fc7b-9c00
The Vendor PN is TXN132241013AS3
BW: 10G, Transceiver Mode: SingleMode
WaveLength: 1310nm, Transmission Distance: 10km
RX Power: -19.75dBm, TX Power: -3.51dBm
Media type: fiber ,loopback: none , Scramble enabled, clock master , WAN full-
du
plex mode ,Pause Flowcontrol:Receive Enable and Send Enable
Flag J0 ""
Flag J1 ""
Flag C2 26(0x1a)
Last physical up time   : -
Last physical down time : 2000-03-17 20:09:54 UTC+08:00
Current system time: 2000-04-03 15:28:35+08:00
Statistics last cleared:never
   Last 300 seconds input rate: 0 bits/sec, 0 packets/sec
```



```
Last 300 seconds output rate: 0 bits/sec, 0 packets/sec
Input: 0 bytes, 0 packets
Output: 0 bytes, 0 packets
Input:
  Unicast: 0 packets, Multicast: 0 packets
  Broadcast: 0 packets, JumboOctets: 0 packets
  CRC: 0 packets, Symbol: 0 packets
  Overrun: 0 packets, InRangeLength: 0 packets
  LongPacket: 0 packets, Jabber: 0 packets
  Fragment: 0 packets, Undersized Frame: 0 packets
  RxPause: 0 packets
Output:
  Unicast: 0 packets, Multicast: 0 packets
  Broadcast: 0 packets, JumboOctets: 0 packets
  System: 0 packets, Overrun: 0 packets
  TxPause: 0 packets
  Unknown Vlan: 0 packets
Input bandwidth utilization  :    0%
Output bandwidth utilization :    0%
```

Recovery measures:

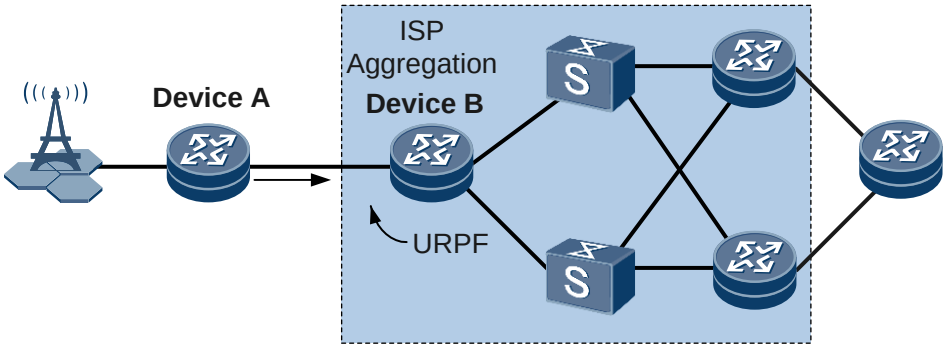
Run the **mtu** *mtu* command in the interface view of the local GE or Eth-Trunk interface that backs up data to set an interface MTU value greater than or equal to 2000 bytes.

1.10.2 URPF Configuration Instructions

1.1.1.1 Configure URPF to Forward Packets Matching the Default Route in Load Balancing Scenarios

Scenario

On the network shown in the following figure, users access an ISP aggregation device (device B) through device A, and URPF is configured on the upstream interface of device A to protect the ISP aggregation device and other devices on the Internet against source address spoofing attacks from user networks.



Configuration Requirements

A traffic policy must be configured on the ISP aggregation device (device B) to allow traffic from a specified network segment to pass the URPF check.

The **ip urpf strict allow-default** command must be run on the upstream interface of device A to configure URPF to forward packets matching the default route.

Misconfiguration Risks

Risk description:

If URPF is not configured to forward packets matching the default route in load balancing scenarios, services are interrupted.

Identification method:

Run the **display current-configuration interface** command in the user view to check URPF configurations. If no **ip urpf strict allow-default** configuration is displayed, the risk exists.

```
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address  192.168.1.1
 ip urpf loose
#
……
```

Recovery measures:

Configure a traffic policy on the ISP aggregation device (device B) to allow traffic from a specified network segment to pass the URPF check. Run the **ip urpf strict allow-default** command on the upstream interface of device A to configure URPF to forward packets matching the default route.

1.11 User access

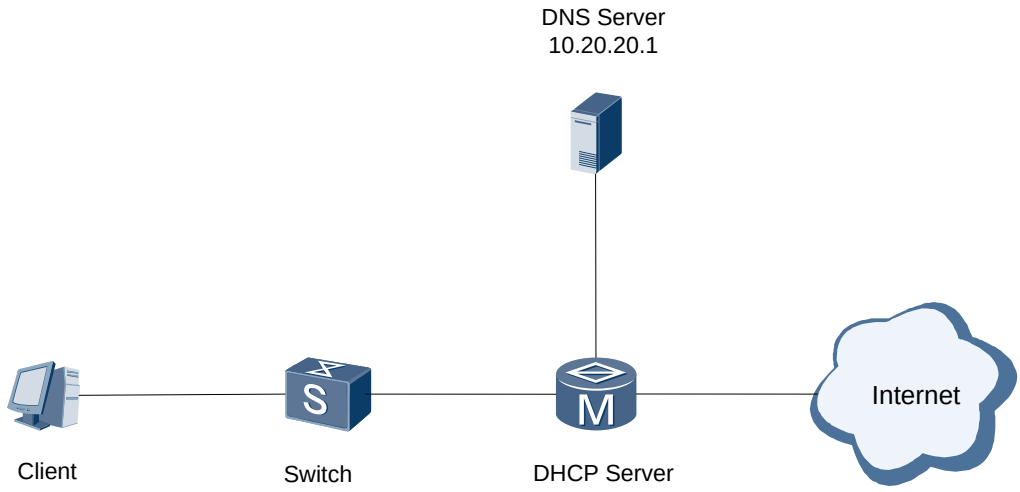
1.11.1 Address Management Configuration Instructions

1.1.1.1 Limit the Number of Connection Requests from DHCP Users to Prevent Traffic Overloads from Affecting Logins of Authorized Users

Scenario

If a large number of invalid DHCP Discover/Request packets exist on a network, the network may be overloaded, and even authorized users may fail to go online.

The following figure shows the networking when a DHCP user goes online.



Configuration Requirements

The **dhcp connection chasten** { **authen-packets** *authen-packets* | **request-packets** *request-packets* } * **check-period** *check-period* **restrain-period** *restrain-period* [**slot** *slotid*] command must be run in the system view to set the parameters to proper values so that the number of DHCP Discover/Request packets sent by DHCP users is limited.

Misconfiguration Risks

Risk description:

The **dhcp connection chasten request-packets *3* check-period *60* restrain-period *180*** command is run in the system view on a device. If a user sends more than three DHCP Discover/Request packets to the device in one minute, the user is suppressed for three minutes during which the packets sent by the user are discarded. The check period of 180s is improperly set, resulting in slow logins of authorized DHCP users.

Identification method:

Run the **display current-configuration** command to query all configurations and check whether the **dhcp connection chasten** command exists.

```
<HUAWEI> display current-configuration # dhcp connection chasten request-packets 3
check-period 60 restrain-period 180 # …
```

Recovery measures:

Two recovery measures are available:

1. Run the **undo dhcp connection chasten** command in the system view to cancel the configuration.
2. Set the parameters to proper values according to the actual situation.

1.11.1.2 Assign an IP Address to a RUI User Who Is Triggered to Go Online Again from the Address Pool Bound to the Domain

Scenario

After a RUI user goes online from the master device, an ARP probe failure causes the user to be logged out. After the user is logged out, the original address pool is deleted and a new address pool is configured. However, the user fails to release the assigned IP address.

Configuration Requirements

None

Misconfiguration Risks

Risk description:

The IP address assigned to the RUI user who is triggered to go online again is not in the newly configured address pool.

Identification method:

None

Recovery measures:

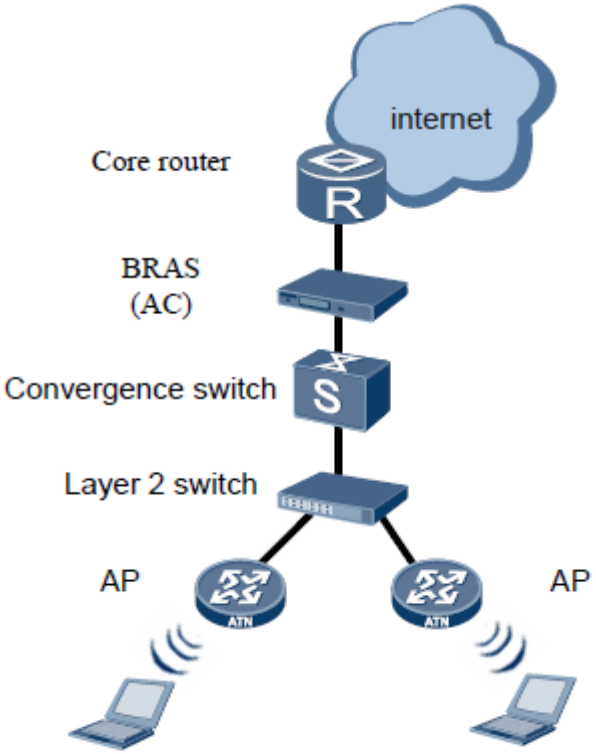
Restart the client to reapply for an IP address, or wait till the lease of the assigned IP address expires and the lease renewal fails. An IP address in the newly configured address pool can be assigned to the user after the user relogs in.

1.11.2 WLAN Roaming Configuration Instructions

Scenario

The AC is connected to APs through a Layer 2 network. Data is directly forwarded as shown in Figure 1-20.

Figure 1-20 Direct data forwarding



Configuration Requirements

In a WLAN roaming scenario, if the physical location information of a terminal changes (the MAC address remains unchanged), the terminal resends DHCP or ND login requests. Determine whether to run the **dhcp session-mismatch action offline** or **dhcp session-mismatch action roam ipv4** command as required.

If you need the device to detect a change in user status immediately after the physical location of a user terminal is changed, the **dhcp session-mismatch action offline** command must be run to log out the online user, so that the user can go online again after resending login requests.

Misconfiguration Risks

Risk description:

In a WLAN scenario, when terminal users roam between non-neighboring hotspots or switch their SSIDs, their physical location information is changed, but their MAC addresses remain unchanged. In this situation, the user terminals resend DHCP login requests. The device treats the resent DHCP or ND login requests as attack packets and discards them because the physical location information of the user terminals is changed, while their MAC addresses remain unchanged. The device considers that the terminal users are still online when they may have gone offline. The device cannot immediately detect user logouts. As a result, the users cannot go online again quickly.

Identification method:

Run the **display current-configuration interface** command in any view to check the configuration of the BAS interface. If neither the **dhcp session-mismatch action offline** command nor the **dhcp session-mismatch action roam ipv4** command is run in the BAS interface view, and only the user access type is configured, the problem may occur.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet2/0/0.77
[HUAWEI-GigabitEthernet2/0/0.77] bas
[HUAWEI-GigabitEthernet2/0/0.77-bas] access-type layer2-subscriber
[HUAWEI-GigabitEthernet2/0/0.77-bas] dhcp session-mismatch action offline
```

Configuration Impact:

By default, the device will not log out online users whose physical location information is changed but MAC addresses remain unchanged when they resend DHCP or ND login requests.

After the **dhcp session-mismatch action offline** command is run, the device will log out terminal users when they resend DHCP or ND login requests. After that, when the users continue to send DHCP or ND login requests, the users can go online again quickly.

NOTE

After the **dhcp session-mismatch action offline** command is run, if an attack source sends DHCP or ND login requests with bogus MAC addresses, online users may be disconnected. This may bring security risks. Therefore, exercise caution when running this command.

Run the **dhcp session-mismatch action roam ipv4** command to configure an interface to use received DHCP Discover or Request messages to trigger roaming procedures for WLAN users who roam to this interface, so that the users can access the network again without re-authentication.

```
[HUAWEI] interface GigabitEthernet2/0/0.77
[HUAWEI-GigabitEthernet2/0/0.77] bas
[HUAWEI-GigabitEthernet2/0/0.77-bas] access-type layer2-subscriber
[HUAWEI-GigabitEthernet2/0/0.77-bas] dhcp session-mismatch action roam ipv4
```

Configuration Impact:

By default, the device directly discards the received DHCP Discover or Request messages from online users whose physical location information is changed but their MAC addresses remain unchanged. After the **dhcp session-mismatch action roam ipv4** command is run, when user terminals whose physical location information is changed resend DHCP login requests, the device will not discard the requests. Instead, the device responds with the terminals' original IP addresses and updates the physical location information of the terminals. This configuration ensures that services are not interrupted.

NOTE

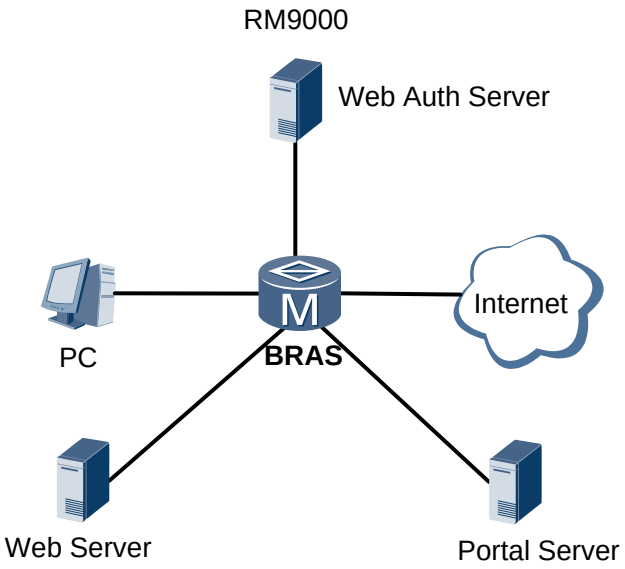
If an attack source sends DHCP access requests with bogus MAC addresses, normal user access traffic may be switched to the attack source so that normal access users cannot access the network. This may bring security risks. Therefore, exercise caution when running this command.

1.11.3 ACL Configuration Instructions

Scenario

Users go online using web authentication.

Figure 1-21 Web user access



Configuration Requirements

1. The **rule** *rule-id* **permit ip source user-group web-before destination ip-address** *ip-address* command must be run in the user ACL view to configure an ACL rule which lists accessible IP addresses for users in the pre-authentication domain. The ACL rule must be bound to a traffic classifier in the traffic classifier view.
2. The **rule** *rule-id* **permit tcp source user-group web-before destination-port eq www** command must be run in the user ACL view to configure an ACL rule based on which TCP packets are filtered. The **http-redirect** command must be run in the traffic behavior view to redirect login users to an authentication web page.

Misconfiguration Risks

Risk description:

None

Recovery measures:

None

1.12 Value-Added Service

1.12.1 DAA Configuration Instructions

1.1.1.1 Bind a Correct VPN Instance to the DAA Service Policy So That NAT Can Be Implemented for Users Configured with the DAA Service

Scenario

NAT needs to be implemented after a user goes online. The DAA service has been configured, but the DAA service policy is not bound to a correct VPN instance.

Configuration Requirements

1. If the DAA service needs to be configured, a user group must be configured for the DAA service policy and a correct VPN instance must be bound to the user DAA service policy.
2. If the value-added service does not need to be configured, the **undo value-added-service policy** command needs to be run in the AAA domain view to delete configurations of the DAA service policy.

Misconfiguration Risks

Risk description:

User traffic matches the rules defined in the DAA service policy, but the DAA service policy is not bound to a correct VPN instance. As a result, traffic fails to be distributed to CGN boards and user packets are discarded.

Identification method:

In the user view, run the **display value-added-service user user-id** *used-id* command to check whether the user is configured with the value-added service. If the command output contains **The used VAS service id table are**, the user is configured with the DAA service.

```
<HUAWEI> display value-added-service user user-id 0
------------------------------------------------------------------------------
 User access index         : 0
 State                    : Used
 User name                : 0000000000ad@zw
 User service number       : 1
 COPS server name          : --
 DAA rate limit mode outbound: --
------------------------------------------------------------------------------
 The used VAS service id table are:
 (    0,    1)
------------------------------------------------------------------------------
------------------------------------------------------------------------------
```

Recovery measures:

1 If the DAA service needs to be configured, configure a user group for the DAA service policy and bind a correct VPN instance to the user DAA service policy.

3. If the DAA service has been activated after the user goes online but the user does not need the DAA service, run the **undo value-added-service policy** command in the AAA domain view to delete configurations of the DAA service policy, and then make the user go online again.

1.13 IPv6 Transition Technologies

1.13.1 CGN Configuration Instructions

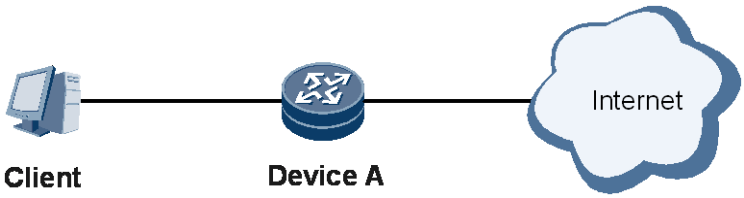
1.1.1.1 Configure CGN Redundancy

When CGN services are configured on a VSUF and no redundancy is configured, users on the VSUF cannot access the network if a fault occurs on the VSUF. To prevent this problem, you must deploy multiple VSUFs and configure CGN service redundancy.

Scenario

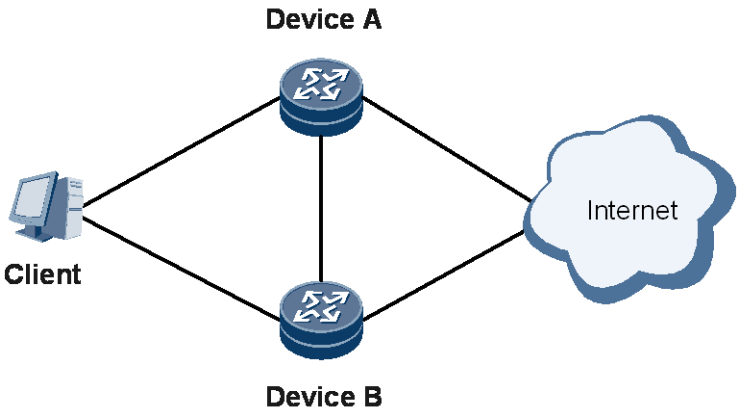
In Figure 1-7, a user accesses the network after user information is converted using CGN on a VSUF installed on device A.

Figure 1-22 User access failure with device A performing CGN translation



Alternatively, in Figure 1-8, a user accesses a network after user information is converted using CGN configured on VSUFs that are installed on device A and device B.

Figure 1-23 User access failure with device A and device B performing CGN translation



Configuration Requirements

Multiple VSUFs must be installed to implement CGN service redundancy. Perform the following operations:

- Configure NAT inter-board hot backup (VSUF-80/160).
- Configure dual-device inter-chassis hot backup (VSUF-80/160).

Misconfiguration Risks

Risk description:

When a CGN service board is faulty and cannot be used, CGN users on the CGN service board cannot access the network.

Identification method:

For VSUFs, CGN services can be backed up in either inter-board or inter-chassis backup mode. The methods for determining risks are as follows:

- To determine the risk of inter-board backup, perform the following steps:
  a. Run the **display device** or **display version slot** *slot-id* command in the user view to check that at least two VSUFs are installed.

```
<HUAWEI> display device
Devicename-X8's Device status:
Slot #    Type      Online    Register     Status     Primary
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1         LPU       Present   Registered   Normal     NA
2         LPU       Present   Registered   Normal     NA
5         VSU       Present   Registered   Normal     NA
8         VSU       Present   Registered   Normal     NA
9         MPU       Present   NA           Normal     Master
10        MPU       Present   Registered   Normal     Slave
11        SFU       Present   Registered   Normal     NA
12        SFU       Present   Registered   Normal     NA
13        SFU       Present   Registered   Normal     NA
14        CLK       Present   Registered   Normal     Master
15        CLK       Present   Registered   Normal     Slave
16        PWR       Present   Registered   Abnormal   NA
17        PWR       Present   Registered   Normal     NA
18        FAN       Present   Registered   Normal     NA
19        FAN       Present   Registered   Normal     NA

<HUAWEI> display version slot 5
VSU 5  : uptime is 2 days, 16 hours, 49 minutes
         StartupTime   2002/07/12   21:46:09
  Host    processor :
  SDRAM Memory Size: 4096M  bytes
  Flash Memory Size:  128M  bytes
  VSU version information
  PCB         Version : CR57VSUF80 REV B
  EPLD        Version : 109
  EPLD2       Version : 106
  EPLD3       Version : 102
  BootROM     Version : 2.30
  BootLoad    Version : 2.19
```



```
  FSURTP     Version : Version 2.1 RELEASE 0372
  FSUKERNEL   Version : Version 2.1 RELEASE 0372
  ASE        Version : 009
  MonitorBUS version information:
  Software    Version : 10.51
  Configure license items:
  2M NAT Session License

<HUAWEI> display version slot 8
VSU 8  : uptime is 0 day, 18 hours, 27 minutes
        StartupTime   2006/07/14   17:13:48
  Host    processor :
  SDRAM Memory Size: 4096M  bytes
  Flash Memory Size:  128M  bytes
  VSU version information
  PCB        Version : CR57VSUF160 REV B
  EPLD       Version : 109
  EPLD2      Version : 106
  EPLD3      Version : 102
  BootROM    Version : 2.30
  BootLoad   Version : 2.19
  FSURTP     Version : Version 2.1 RELEASE 0372
  FSUKERNEL   Version : Version 2.1 RELEASE 0372
  ASE        Version : 009
  MonitorBUS version information:
  Software    Version : 10.51
  Configure license items:
  2M NAT Session License
  20G NAT BandWidth License
```

b. Run the **display nat instance** command in the user view and check information about the bound service instance group. Run the **display service-instance-group** [*group-name*] command and check information about the bound service location. Run the **display service-location** [*service-location-id*] command and check whether the **Backup slot ID** field value exists. If a value exists, inter-board backup is available. If the value is empty, no inter-board backup is provided.

```
<HUAWEI> display nat instance
nat instance dtest id 22
 port-range 4096
 service-instance-group dtest
 nat address-group dtest group-id 22
   section 0 10.100.100.0 mask 255.255.255.0
 nat outbound 2222 address-group dtest

<HUAWEI>display service-instance-group
service-instance-group dtest

<HUAWEI> display service-location
service-location 58
 Location slot ID: 5 engine ID: 0
 Current location slot ID: 5 engine ID: 0
 Backup slot ID: 8 engine ID: 0
 Current backup slot ID: 8 engine ID: 0
 Bound service-instance-group number: 1
```



```
Batch-backup state: finished
```

- To determine the risk of inter-chassis backup, perform the following operations:

  Run the **display nat instance** command in the user view and check information about the bound service instance group. Run the **display service-instance-group** [*group-name*] command and check information about the bound service location. Then run the **display service-location** [*service-location-id*] command and check whether the **Remote-backup interface** field exists. If a value exists, inter-board backup is available. If the value is empty, no inter-board backup is provided.

```
<HUAWEI> display service-location 22
service-location 22
 Backup scene type: inter-box
 Location slot ID: 5 engine ID: 0
 Remote-backup interface: GigabitEthernet2/2/1.1
 Peer: 10.255.255.2
 Vrrp ID: 22
 Vrrp bind interface: GigabitEthernet2/2/1.1
 Vrrp state: master
 Bound service-instance-group number: 1
 Batch-backup state: finished
```

Recovery measures:

Deploy multiple VSUFs and configure CGN service redundancy.

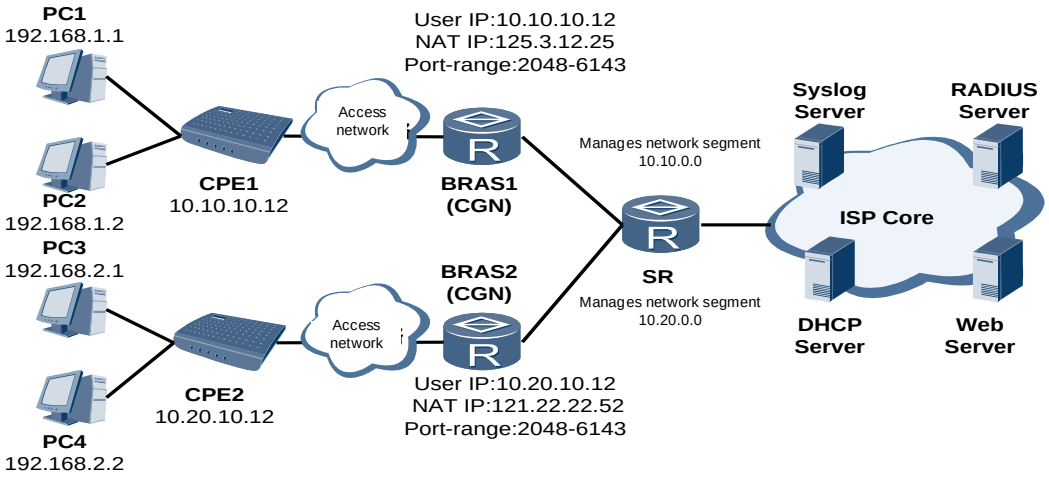
1.13.1.2 Configure a Port Range and the 3-Tuple Mode in a CGN Scenario

In a NAT instance, the number of ports in a port range is set to 1024 for port pre-allocation, and the 5-tuple mode is used for NAT address pool translation. When some users open websites, NAT sessions cannot be established due to insufficient ports.

Scenario

In Figure 1-24, the CPE dials up to a BRAS (with the CGN function integrated) to go online in a distributed CGN scenario. The BRAS assigns the CPE an access IP address and the IP address and port range into which NAT converts original IP address and port number, respectively. When a PC initiates an access request, the CPE performs NAT conversion for the packet sent by the PC. A BRAS performs NAT conversion again for the packet sent by the CPE. This is because NAT is performed twice on the network and the CGN function is deployed on each BRAS.

Figure 1-24 NAT session establishment failure in distributed NAT444 in port pre-allocation mode



Configuration Requirements

In NAT, DS-Lite, or NAT64 instances, to prevent attacks, you must run the **port-range** command to configure the port pre-allocation function. After port pre-allocation is configured, the number of ports that can be assigned to a user is fixed. To conserve ports and meet P2P application requirements, you must configure the 3-tuple mode for the NAT address pools.

A range of port pre-allocation is configured in the NAT, DS-Lite, or NAT64 instances. When NAT is deployed on the live network, the number of ports in a port pre-allocation range is at least 2048. If the number of ports in the port pre-allocation range is less than 2048, you must configure the semi-dynamic port allocation mode. A NAT instance is used as an example. The configuration requirements for port pre-allocation are as follows:

1 Configure a port allocation mode:

- Configure the port pre-allocation mode. For example:

```
nat instance nat444-rui id 1
 port-range 4096
```

- Configure the semi-dynamic port allocation mode in the instance. For example:

```
nat instance nat444-rui id 1
 port-range 1024 extended-port-range 1024 extended-times 1
```

2. Configure the 3-tuple mode in an instance.

```
nat instance nat444-rui id 1
 nat filter mode full-cone
```

Misconfiguration Risks

Risk description:

When the **port-range** *initial-port-range* command is run to set an initial range for port pre-allocation to a value less than 2048 and the 5-tuple mode is used in an instance, NAT sessions fail to be established for some users who attempt to access websites because of insufficient ports.

Identification method:

1 Run the **display nat instance**, **display ds-lite instance**, or **display nat64 instance** command in any view and check instance configurations. Check the **port-range** command in the output to determine whether the number of ports in the port pre-allocation range is less than 2048.

3. Run the **display this** command in the instance view and check whether the 3-tuple mode is configured for the instance.

   If the number of ports in a port pre-allocation range is less than 2048 and the 3-tuple mode is not configured in the instance, some users cannot establish NAT sessions because of insufficient ports.

Recovery measures:

Run the **port-range initial-port-range** command in the instance view to change the port pre-allocation range to 2048 or larger, and run the **nat filter mode full-cone** command in the instance view to enable the 3-tuple mode for the NAT address pool.

2 Deployment Instructions

About This Chapter

NOTE

This document describes the deployment instructions of NE series routers in some scenarios. When configuring and maintaining some features on NE series routers, customers must deploy services according to the deployment instructions to prevent service interruptions caused by incorrect configurations, incorrect use, or missing reliability.

2.1 Configure Redundancy Backup on the User Access Side

A reliability solution must be deployed in user access scenarios. Without a reliability solution, in case of a fault on a link (including optical modules and fibers), interface, board, or device on the access side, services are interrupted due to the lack of backup.

2.2 Configure Redundancy Backup for Network-side Links

Multiple inter-board uplinks on GE interfaces or inter-board uplinks on Eth-Trunk interfaces must be configured for network-side links. If such reliability deployment is not configured, services may be interrupted if interface, link, or board faults occur.

2.3 Configure Redundancy Backup in Scenarios Where the Router Interconnects with Servers

2.4 Configure an RBS to Track a Network-Side Interface in a Dual-Device Hot Backup Scenario

If a remote backup service (RBS) is not configured to track a network-side interface in a dual-device hot backup scenario, the network-side link bandwidth may be insufficient.

2.5 Configure Redundancy Backup for CGN

CGN services are configured on a VSUF or VSUI. When redundancy backup is not configured and the VSUF/VSUI fails, users carried on the VSUF/VSUI cannot access the Internet. To prevent such a problem, deploy multiple VSUFs or VSUIs and configure CGN redundancy.

2.6 Configure Redundancy Backup for GRE Tunnels

2.7 Configure Redundancy Backup for L2TP Tunnels

2.1 Configure Redundancy Backup on the User Access Side

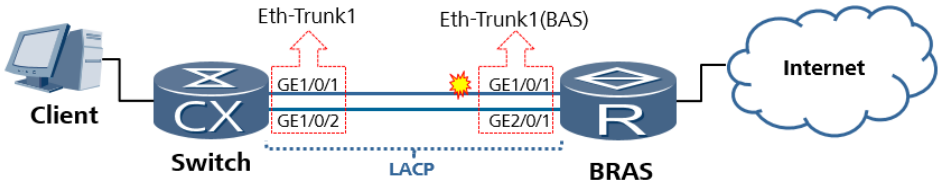
A reliability solution must be deployed in user access scenarios. Without a reliability solution, in case of a fault on a link (including optical modules and fibers), interface, board, or device on the access side, services are interrupted due to the lack of backup.

Scenario

Redundancy backup on the user access side involves three scenarios: inter-board Eth-Trunk hot backup, cold backup for delayed response, and RUI multi-device hot backup. A single device must be configured with inter-board Eth-Trunk hot backup or cold backup for delayed response. RUI multi-device hot backup or cold backup for delayed response can be used for inter-device backup, and inter-device backup must be used for important nodes.

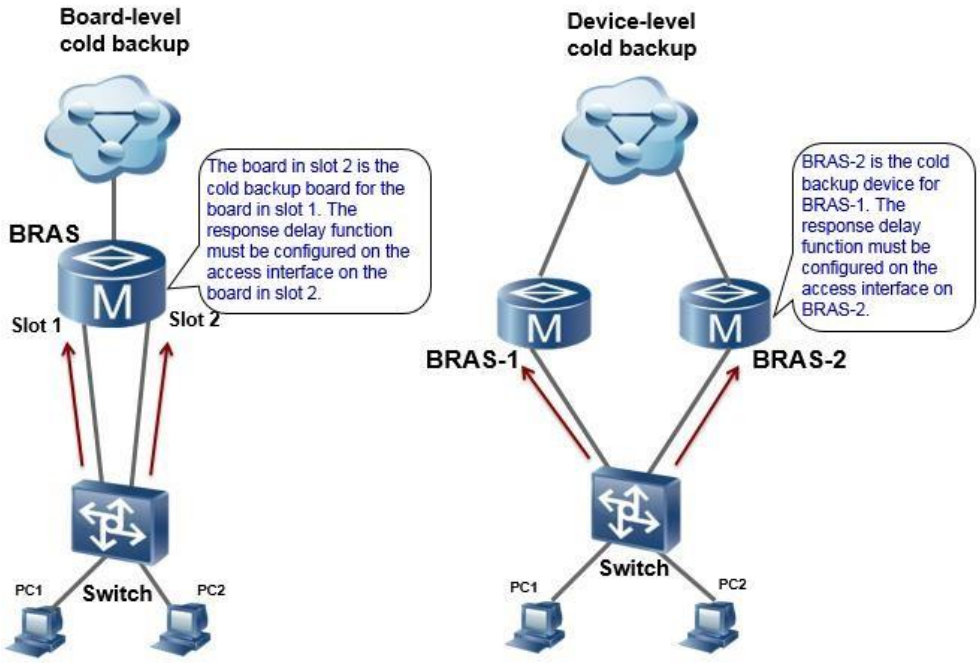
- Inter-board Eth-Trunk hot backup: is based on the fact that Eth-Trunk member interfaces reside on different interface boards, which prevents a member interface fault, link failure, or member interface board fault from causing a traffic interruption, therefore improving user access reliability.

  Figure 2-1 Inter-board Eth-Trunk hot backup

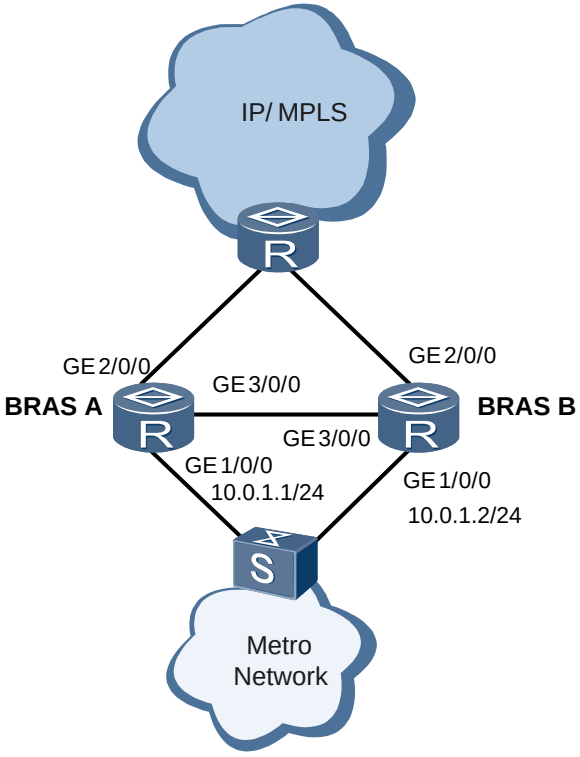
- Cold backup for delayed response: After a response delay policy for user access is configured on a BAS interface, the device extends the response time of the first packet of the user who goes online through the interface according to the configured policy. In addition, multiple interfaces of the downstream access device are required to broadcast the user's access packets. Cold backup for delayed response can be classified into board-level cold backup and device-level cold backup based on deployment scenarios.

Figure 2-2 Delayed response to cold backup



- RUI multi-device hot backup: implements device-level hot backup through real-time user information backup between devices, preventing user disconnection or service interruption caused by link, board, or device faults. For details, see section "Configuring Multi-Device Backup for BRAS User Information" in the product documentation.

Figure 2-3 RUI multi-device hot backup



Configuration Requirements

- **Inter-board Eth-Trunk hot backup**

  When configuring an access-side interface, you must use an inter-board Eth-Trunk interface. The Eth-Trunk interface must contain at least two member interfaces of different member boards. This prevents network accidents, such as traffic interruption, caused by faults on member interfaces or links of the Eth-Trunk interface or the board where the member interfaces reside. This feature improves user access reliability. In addition, user traffic can be load balanced among member boards of an Eth-Trunk interface. For details, see "Configuring an Eth-Trunk Interface in Inter-Board Port Backup Mode" in the product documentation.

- **Cold backup for delayed response**

  Inter-board cold backup for delayed response is classified into board-level cold backup and device-level cold backup. The **access-delay** *delay-time* [**circuit-id-include** *access-node-id* | **even-mac** | **odd-mac**] command is used to configure a response delay policy for user access on the BAS interfaces between two boards or devices that back up each other.

  Configuration example of cold backup for delayed response:

```
[HUAWEI] interface GigabitEthernet 1/0/9.1
[HUAWEI-GigabitEthernet 1/0/9] user-vlan 55
[HUAWEI-GigabitEthernet 1/0/9-vlan-55-55] bas
[HUAWEI-GigabitEthernet 1/0/9-bas] access-type layer2-subscriber
[HUAWEI-GigabitEthernet 1/0/9-bas] authentication-method ppp
[HUAWEI-GigabitEthernet 1/0/9-bas] access-delay 500 odd-mac
[HUAWEI-GigabitEthernet 1/0/9-bas] quit
[HUAWEI] interface GigabitEthernet 2/1/4.1
[HUAWEI-GigabitEthernet 2/1/4] user-vlan 55
[HUAWEI-GigabitEthernet 2/1/4-vlan-55-55] bas
[HUAWEI-GigabitEthernet 2/1/4-bas] access-type layer2-subscriber
[HUAWEI-GigabitEthernet 2/1/4-bas] authentication-method ppp
[HUAWEI-GigabitEthernet 1/0/9-bas] access-delay 500 even-mac
[HUAWEI-GigabitEthernet 2/1/4-bas] quit
```

- **RUI multi-device hot backup**

  Configure RUI multi-device backup on the device, such as the remote backup service and remote backup profile, and bind the remote backup profile to the user access interface. For details, see "Configuring Multi-Device Backup for BRAS User Information" and "Example for Configuring Multi-Device Backup" in the product documentation.

Misconfiguration Risks

- **Inter-board Eth-Trunk hot backup**

  Risk description:

  When the access-side interface is not an inter-board Eth-Trunk interface, if a member interface or link, or the board where a member interface resides is faulty, no reliability backup is available. As a result, users go offline and traffic is interrupted.

  Identification method:

  - If the access-side interface is a common GE interface or sub-interface, configure an inter-board Eth-Trunk interface as the access-side interface.

- If the access-side interface is an Eth-Trunk interface whose member interfaces reside on the same board, configure an inter-board Eth-Trunk interface as the access-side interface.

  Run the following command to view the interface information:

```
[HUAWEI] display eth-trunk
Eth-Trunk10's state information is:
WorkingMode: NORMAL       Hash arithmetic: According to flow
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 16
Operate status: up        Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
----
  PortName               Status     Weight
  GigabitEthernet1/1/1        Up         1
```

- **Cold backup for delayed response**

  Risk description:

  If no backup board or device is available on the network, if the interface, board, or device used for user access is faulty, no backup link is available for the user to go online. As a result, services cannot be restored in time after the user goes offline, and the traffic is interrupted.

  Identification method:

  - Check whether the access network meets the networking requirements of cold backup for delayed response. For details, see the network topology.
  - Then, check whether the **access-delay** *delay-time* [**circuit-id-include** *access-node-id* | **even-mac** | **odd-mac**] command is configured on the BAS interface of the backup board or device.

- **RUI multi-device hot backup**

  Risk description:

  When a fault occurs on the access-side link, network-side link, board, or entire device of BRAS A, user information is not backed up to BRAS B. As a result, users go offline, and network access fails.

  Identification method:

  - Check whether the remote backup service and remote backup profile are configured on the device.
  - Run the **display remote-backup-profile** and **display remote-backup-service** commands to check whether the remote backup profile and remote backup service are configured correctly, respectively. Then check whether user information is backed up after users go online.

  After configuring the remote backup profile, run the **display remote-backup-profile** command. The remote backup service type is **bras**. The remote backup profile named **profile1** is bound to **GigabitEthernet1/0/0.1** from which users attempt to go online. Device A is in the **Master** state.

```
<HUAWEI-A> display remote-backup-profile profile1
-----------------------------------------------
 Profile-Index       : 0x802
 Profile-Name        : profile1
 Service            : bras
 Remote-backup-service: service1
 Backup-ID          : 10
 track protocol      : VRRP
 VRRP-ID            : 1
```



```
VRRP-Interface      : GigabitEthernet1/0/0.2
Access-Control      : Even-Mac
State              : Master
Peer-state          : Slave
VRRP-ID            : 2
VRRP-Interface      : GigabitEthernet1/0/0.3
Access-Control      : Odd-Mac
State              : Slave
Peer-state          : Master
Interface          :
                   GigabitEthernet1/0/0.1
Backup mode         : hot
Slot-Number         : 1
Card-Number         : 0
Port-Number         : 0
Nas logic-port      : Gigabitethernet 1/0/0
Nas logic-ip        : 10.2.3.4
Nas logic-sysname    : huawei
Traffic interval    : 10(minutes)
```

After configuring the remote backup service, run the **display remote-backup-service** command. The TCP connection is in the **Connected** state.

```
<HUAWEI-A> display remote-backup-service service1
-------------------------------------------------------------
 Service-Index    : 0
 Service-Name     : service1
 TCP-State        : Connected
 Peer-ip          : 10.88.88.88
 Source-ip        : 10.22.22.22
 TCP-Port         : 2046
 Track-BFD        : --
 Track-interface0 : GigabitEthernet2/0/0
 Track-interface1 : --
-------------------------------------------------------------
......
```

After users go online, run the **display backup-user** command to view user information that is backed up.

```
<HUAWEI> display backup-user
  Remote-backup-service: service1
  Total Users Numer: 10
------------------------------------------------------------------------------
 100    101    102    103    104    105    106    107    108    109
------------------------------------------------------------------------------
```

Recovery measures:

See the configuration requirements.

2.2 Configure Redundancy Backup for Network-side Links

Multiple inter-board uplinks on GE interfaces or inter-board uplinks on Eth-Trunk interfaces must be configured for network-side links. If such reliability deployment is not configured, services may be interrupted if interface, link, or board faults occur.

Scenario

Reliability deployment is configured for network-side links. The reliability deployment can be configured on GE or Eth-Trunk interfaces, or in a single- or multi-uplink scenarios. The main purpose is to back up forwarding routes to ensure continuity of user-to-network services.

Configuration Requirements

Network-side links are configured as multiple inter-board uplinks on GE interfaces or inter-board uplinks on Eth-Trunk interfaces.

Misconfiguration Risks

Risk description:

If network-side links are not backed up, user service traffic may be interrupted if interface, link, or board faults occur.

Identification method:

1. Run the **display ip routing-table** command to check that the default route or each network-side specific route has at least two outbound interfaces.
2. Check whether the route has multiple outbound interfaces residing on different boards.

Recovery measures:

See the configuration requirements.

2.3 Configure Redundancy Backup in Scenarios Where the Router Interconnects with Servers

Scenario

In the scenario where a router interconnects with DHCP, RADIUS, web, Diameter, or DNS servers, redundancy backup needs to be configured for the servers to ensure that communication with the servers is not affected if the servers become faulty or unreachable.

Configuration Requirements

- Redundancy backup must be configured on the servers. For example, multiple servers are deployed or the servers work in load balancing mode.
- Multiple IP addresses must be configured for each type of server on the router to implement redundancy backup in master/backup or load balancing mode.

Misconfiguration Risks

Risk description:

If no redundancy backup is configured on the servers, services may be interrupted if the router fails to communicate with the servers.

If a router is not configured with the master/slave or load balancing mode and the communication between the router and a server is faulty, the router cannot automatically switch services. As a result, services are affected.

Identification method:

Check whether multiple IP addresses are configured for the servers on the router. For details, see "Configuring RADIUS Authentication and Accounting Servers" and "Configuring a DHCPv4 Server Group."

Recovery measures:

Configure redundancy backup in scenarios where the router interconnects with servers.

2.4 Configure an RBS to Track a Network-Side Interface in a Dual-Device Hot Backup Scenario

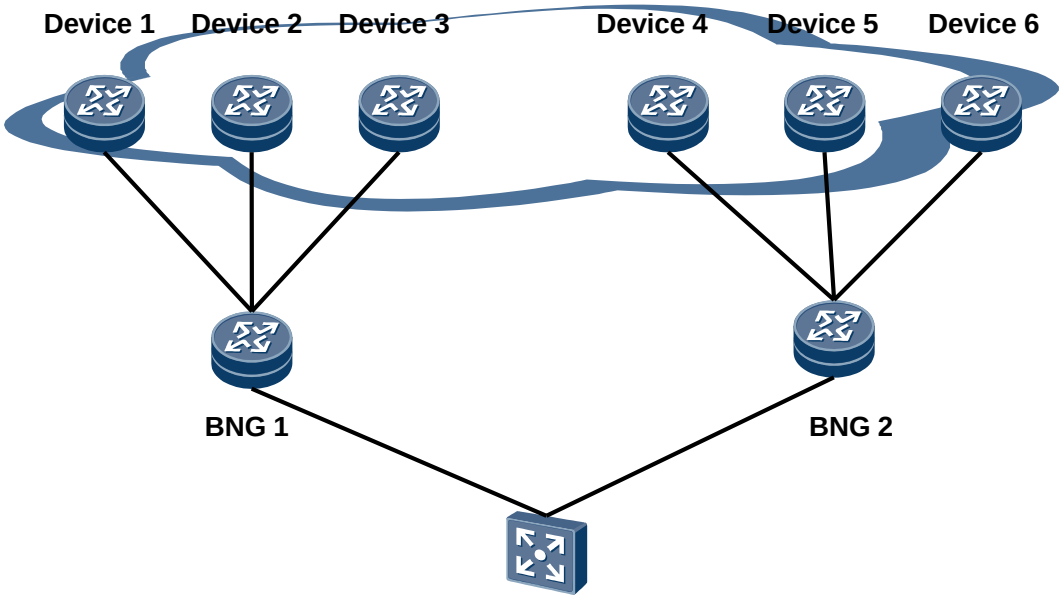
If a remote backup service (RBS) is not configured to track a network-side interface in a dual-device hot backup scenario, the network-side link bandwidth may be insufficient.

Scenario

An RBS is a general backup module and uses TCP as the transmission protocol. The RBS provides registration interfaces for other service modules and batch backup and real-time backup. After a TCP connection is established, the RBS uses a backup protocol to back up data in batches or in real time. A remote backup profile (RBP) provides a user interface for configuring multi-device backup.

When configuring an RBS, check whether the TCP connection established for the RBS fails and whether the fault is rectified.

Figure 2-4 Dual-device hot backup networking



Configuration Requirements

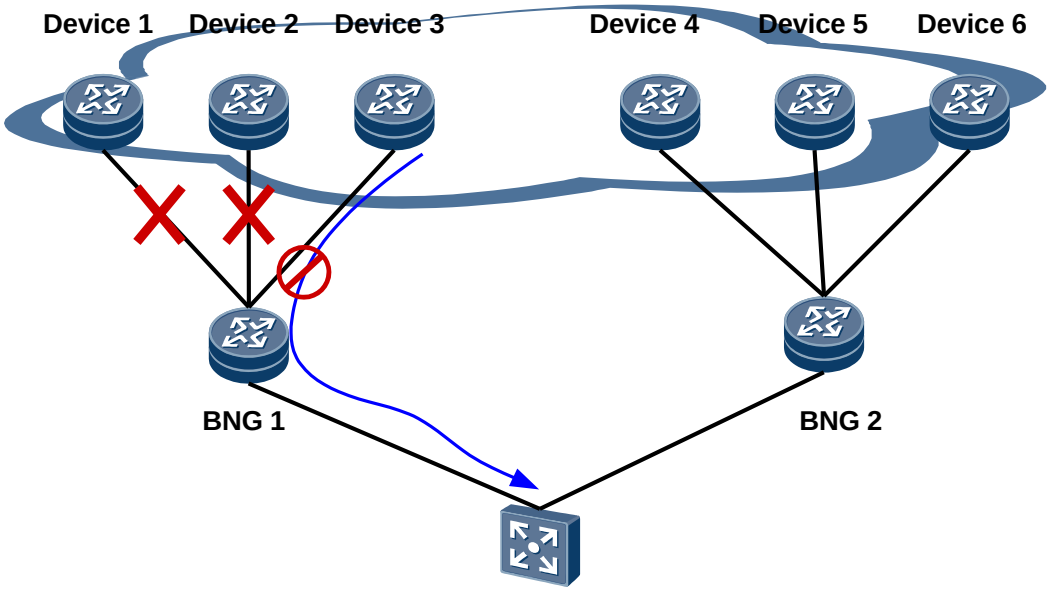
1 When an RBS is configured, the **track interface** *interface-name* [**weight** *weight*] command must be run to configure the RBS to track a network-side interface. This configuration is used to check whether the TCP connection established for the RBS fails and whether the fault is rectified.

2. The **switchover uplink** { **failure-ratio** *failure-ratio* | **duration** *duration* } * command must be run to configure a threshold for a master/backup switchover caused by uplink failures and a duration before the switchover. This configuration controls the withdrawal of address pool routes bound to the RBS.

Misconfiguration Risks

Risk description:

Figure 2-5 Dual-device hot backup networking



If BNG1's multiple network-side interfaces fail, traffic cannot be switched to BNG2 because the RBS fails to detect the status of the network-side interfaces. BNG1 has only one working link, which causes the network-side link bandwidth to be insufficient. As a result, the network may not work properly.

Identification method:

- Obtain the name of a network-side interface. For details, see the network topology.
- Run the **display remote-backup-service** *rbs-name* field in the command output. The following command output indicates that the RBS named **hw** has tracked the network-side interface **GigabitEthernet2/0/5**.

```
[HUAWEI] display remote-backup-service hw
------------------------------------------------------------
Service-Index    : 1
Service-Name     : hw
TCP-State        : Connected
Peer-ip          : 10.1.1.2
Source-ip        : 10.1.1.1
TCP-Port         : 6001
Track-BFD        : --
Track-interface0 : GigabitEthernet2/0/5
Weight : 10
Uplink state     : 2 (1:DOWN 2:UP)
Last up time     : 2006-07-28 10:36:16
Last down time   : 2006-07-28 10:33:50
Last down reason : TCP closed for echo time out.
Domain-map-list  : --
```

Recovery measures:

Configure an RBS to track a network-side interface in a dual-device hot backup scenario.

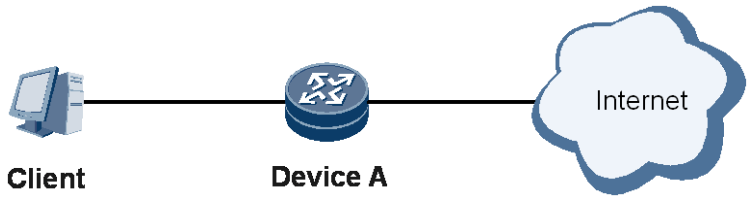
2.5 Configure Redundancy Backup for CGN

CGN services are configured on a VSUF. When redundancy backup is not configured and the VSUF fails, users carried on the VSUF cannot access the Internet. To prevent such a problem, deploy multiple VSUFs and configure CGN redundancy.

Scenario

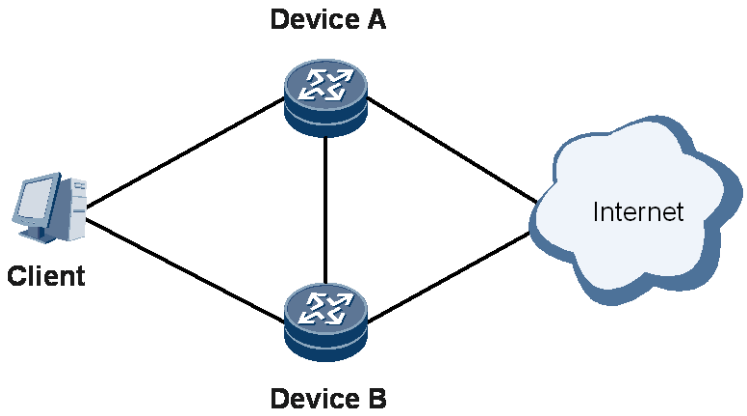
On the network shown in Figure 2-6, the user accesses the Internet after Device A with a VSUF installed performs CGN translation.

Figure 2-6 User access to the Internet after Device A performs CGN translation



On the network shown in Figure 2-7, alternatively, the user accesses the Internet after Device A and Device B with a VSUF installed perform CGN translation.

Figure 2-7 User access to the Internet after Device A and Device B perform CGN translation



Configuration Requirements

When CGN services are configured on a VSUF, multiple VSUFs need to be deployed to implement CGN service redundancy. For details about the operations, see:

- Configure inter-board NAT hot backup (VSUF-80/160)
- Configure dual-device inter-chassis NAT hot backup (VSUF-80/160)

Misconfiguration Risks

Risk description:

CGN users carried on the faulty VSUF cannot access the Internet.

Identification method:

For VSUFs, redundancy backup modes for CGN services are classified as inter-board backup or inter-chassis backup.

- To determine the risk of inter-board backup, perform the following steps:
  a. Run the **display device** or **display version slot** *slot-id* command in the user view to check that at least two VSUFs are available.

```
<HUAWEI> display device
Devicename-X8's Device status:
Slot #   Type     Online   Register     Status     Primary
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
-
1        LPU      Present   Registered   Normal     NA
2        LPU      Present   Registered   Normal     NA
5       VSU     Present   Registered   Normal     NA
8       VSU     Present   Registered   Normal     NA
9        MPU      Present   NA          Normal     Master
10       MPU      Present   Registered   Normal     Slave
11       SFU      Present   Registered   Normal     NA
12       SFU      Present   Registered   Normal     NA
13       SFU      Present   Registered   Normal     NA
14       CLK      Present   Registered   Normal     Master
15       CLK      Present   Registered   Normal     Slave
16       PWR      Present   Registered   Abnormal   NA
17       PWR      Present   Registered   Normal     NA
18       FAN      Present   Registered   Normal     NA
19       FAN      Present   Registered   Normal     NA

<HUAWEI> display version slot 5
VSU 5  : uptime is 2 days, 16 hours, 49 minutes
       StartupTime  2002/07/12  21:46:09
  Host   processor :
  SDRAM Memory Size: 4096M  bytes
  Flash Memory Size:  128M  bytes
  VSU version information
  PCB        Version : CR57VSUF80 REV B
  EPLD       Version : 109
  EPLD2      Version : 106
  EPLD3      Version : 102
  BootROM    Version : 2.30
  BootLoad   Version : 2.19
  FSURTP     Version : Version 2.1 RELEASE 0372
  FSUKERNEL  Version : Version 2.1 RELEASE 0372
  ASE        Version : 009
  MonitorBUS version information:
  Software   Version : 10.51
  Configure license items:
  2M NAT Session License

<HUAWEI> display version slot 8
VSU 8  : uptime is 0 day, 18 hours, 27 minutes
       StartupTime  2006/07/14  17:13:48
  Host   processor :
```



```
 SDRAM Memory Size: 4096M  bytes
 Flash Memory Size:  128M  bytes
 VSU version information
 PCB        Version : CR57VSUF160 REV B
 EPLD       Version : 109
 EPLD2      Version : 106
 EPLD3      Version : 102
 BootROM    Version : 2.30
 BootLoad   Version : 2.19
 FSURTP     Version : Version 2.1 RELEASE 0372
 FSUKERNEL  Version : Version 2.1 RELEASE 0372
 ASE        Version : 009
 MonitorBUS version information:
 Software   Version : 10.51
 Configure license items:
 2M NAT Session License
 20G NAT BandWidth License
```

b. Run the **display nat instance** command in the user view to check the bound **service-location.** Then run the **display service-location** [*service-location-id*] command to check whether the **Backup slot ID** field exists. If the **Backup slot ID** field exists, inter-board backup has been configured. If the **Backup slot ID** field does not exist, inter-board backup has not been configured.

```
<HUAWEI> display nat instance
nat instance dtest id 22
 port-range 4096
 service-instance-group dtest
 nat address-group dtest group-id 22
   section 0 10.100.100.0 mask 255.255.255.0
 nat outbound 2222 address-group dtest

<HUAWEI> display service-location
service-location 58
 Location slot ID: 5 engine ID: 0
 Current location slot ID: 5 engine ID: 0
 Backup slot ID: 8 engine ID: 0
 Current backup slot ID: 8 engine ID: 0
 Bound service-instance-group number: 1
 Batch-backup state: finished
```

- To determine the risk of inter-chassis backup, perform the following steps:

  Run the **display nat instance** command in the user view to check the bound **service-location.** Then run the **display service-location** [*service-location-id*] command to check whether the **Remote-backup interface** field exists. If the **Remote-backup interface** field exists, inter-chassis backup has been configured. If the **Remote-backup interface** field does not exist, inter-chassis backup has not been configured.

```
<HUAWEI> display service-location 22
service-location 22
 Backup scene type: inter-box
 Location slot ID: 5 engine ID: 0
 Remote-backup interface: GigabitEthernet2/2/1.1
 Peer: 10.255.255.2
 Vrrp ID: 22
 Vrrp bind interface: GigabitEthernet2/2/1.1
```



```
Vrrp state: master
Bound service-instance-group number: 1
Batch-backup state: finished
```

Recovery measures:

Configure redundancy backup for CGN.

2.6 Configure Redundancy Backup for GRE Tunnels

Scenario

GRE tunnels are used.

Configuration Requirements

If multiple tunnel service boards are configured on a device, the **target-board** *slot-number* **backup** *slot-number2* command must be run to configure 1:1 protection for GRE tunnels, enhancing GRE service reliability. After 1:1 protection is configured for GRE tunnel service boards, configure two GRE tunnels with the same source and destination on the master and slave GRE tunnel service boards. When the GRE tunnel on the master GRE tunnel service board is working, the GRE tunnel on the slave GRE tunnel service board does not work. If the master GRE tunnel service board fails, services are switched to the GRE tunnel on the slave GRE tunnel service board. For configuration details, see "GRE Configuration."

Misconfiguration Risks

Risk description:

If a board carrying GRE services fails, the GRE services are interrupted.

Identification method:

Run the **display tunnel gre backup** command to check GRE tunnel backup binding information. If **Tunnel binding slave slot** does not exist, no slave GRE tunnel service board is configured.

```
<HUAWEI> display tunnel gre backup
GRE tunnel backup binding information:
Tunnel binding master slot:  1
Tunnel binding slave slot:   2
Tunnel processing slot:      1
```

Recovery measures:

Configure redundancy backup for GRE tunnels.

2.7 Configure Redundancy Backup for L2TP Tunnels

Scenario

L2TP tunnels are used.

Configuration Requirements

Multiple tunnel service boards can be specified for an LNS group. Load balancing is implemented among these tunnel service boards based on tunnels. If multiple tunnel service boards are configured on a device, the **bind slot** *slot-id* command must be run in the LNS group view to bind two or more tunnel service boards to the LNS group to implement backup. For configuration details, see "Setting Tunnel Parameters on the LNS."

Misconfiguration Risks

Risk description:

If a board carrying L2TP services fails, the L2TP services are interrupted.

Identification method:

Run the **display lns-group all** command to check the interfaces and tunnel service boards bound to LNS groups. If only one tunnel service board is bound to an LNS group, no slave tunnel service board is configured.

```
<HUAWEI> display lns-group all
-------------------------------------------------------
 GroupNum GroupName    Interface            AllSlot
 0         lns1        Loopback0             ----
 1         test        Loopback1            2
 -------------------------------------------------------
```

Recovery measures:

Configure redundancy backup for L2TP tunnels.

