HP 5500 EI & 5500 SI Switch Series

High Availability

Configuration Guide

Part number: 5998-1709

Software version: Release 2220

Document version: 6W100-20130810

Legal and notice information

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Contents

High availability overview

Communication interruptions can seriously affect widely-deployed value-added services such as IPTV and video conference. Therefore, the basic network infrastructures must be able to provide high availability.

The following are the effective ways to improve availability:

- Increasing fault tolerance
- Speeding up fault recovery
- Reducing impact of faults on services

Availability requirements

Availability requirements fall into three levels based on purpose and implementation.

Table 1 Availability requirements

Level	Requirement	Solution
1	Decrease system software and hardware faults	• **Hardware**—Simplifying circuit design, enhancing production techniques, and performing reliability tests. • **Software**—Reliability design and test
2	Protect system functions from being affected if faults occur	Device and link redundancy and deployment of switchover strategies
3	Enable the system to recover as fast as possible	Performing fault detection, diagnosis, isolation, and recovery technologies

The level 1 availability requirement should be considered during the design and production process of network devices. Level 2 should be considered during network design. Level 3 should be considered during network deployment, according to the network infrastructure and service characteristics.

Availability evaluation

Mean Time Between Failures (MTBF) and Mean Time to Repair (MTTR) are used to evaluate the availability of a network.

MTBF

MTBF is the predicted elapsed time between inherent failures of a system during operation. It is typically in the unit of hours. A higher MTBF means a high availability.

MTTR

MTTR is the average time required to repair a failed system. MTTR in a broad sense also involves spare parts management and customer services.

MTTR = fault detection time + hardware replacement time + system initialization time + link recovery time + routing time + forwarding recovery time. A smaller value of each item means a smaller MTTR and a higher availability.

High availability technologies

Increasing MTBF or decreasing MTTR can enhance the availability of a network. The high availability technologies described in this section meet the level 2 and level 3 high availability requirements by decreasing MTTR.

High availability technologies can be classified as fault detection technologies or protection switchover technologies.

Fault detection technologies

Fault detection technologies enable detection and diagnosis of network faults. CFD, DLDP, and Ethernet OAM are data link layer fault detection technologies. BFD is a generic fault detection technology that can be used at any layer. NQA is used for diagnosis and evaluation of network quality. Monitor Link and Track work along with other high availability technologies to detect faults through a collaboration mechanism.

Table 2 Fault detection technologies

Technology	Introduction	Reference
CFD	Connectivity Fault Detection (CFD), which conforms to IEEE 802.1ag Connectivity Fault Management (CFM) and ITU-T Y.1731, is an end-to-end per-VLAN link layer Operations, Administration and Maintenance (OAM) mechanism used for link connectivity detection, fault verification, and fault location.	"Configuring CFD" in *High Availability Configuration Guide*
DLDP	The Device link detection protocol (DLDP) deals with unidirectional links that may occur in a network. Upon detecting a unidirectional link, DLDP, as configured, can shut down the related port automatically or prompt users to take actions to avoid network problems.	"Configuring DLDP" in *High Availability Configuration Guide*
Ethernet OAM	As a tool monitoring Layer 2 link status, Ethernet OAM is mainly used to address common link-related issues on the "last mile". You can monitor the status of the point-to-point link between two directly connected devices by enabling Ethernet OAM on them.	"Configuring Ethernet OAM" in *High Availability Configuration Guide*
BFD (available only on the HP 5500 EI)	Bidirectional forwarding detection (BFD) provides a single mechanism to quickly detect and monitor the connectivity of links or IP forwarding in networks. To improve network performance, devices must quickly detect communication failures to restore communication through backup paths as soon as possible.	"Configuring BFD" in *High Availability Configuration Guide*
NQA	Network Quality Analyzer (NQA) analyzes network performance, services and service quality through sending test packets, and provides you with network performance and service quality parameters such as jitter, TCP connection delay, FTP connection delay and file transfer rate.	"Configuring NQA" in *Network Management and Monitoring Configuration Guide*
Monitor Link	Monitor Link works together with Layer 2 topology protocols to adapt the up/down state of a downlink port to the state of an uplink port. This feature enables fast link switchover on a downstream device in response to the uplink state change on its upstream device.	"Configuring Monitor Link" in *High Availability Configuration Guide*

Technology	Introduction	Reference
Track	The track module is used to implement collaboration between different modules. The collaboration here involves three parts: the application modules, the track module, and the detection modules. These modules collaborate with one another through collaboration entries. That is, the detection modules trigger the application modules to perform certain operations through the track module. More specifically, the detection modules probe the link status, network performance and so on, and inform the application modules of the detection result through the track module. Once notified of network status changes, the application modules deal with the changes to avoid communication interruption and network performance degradation.	"Configuring track" in *High Availability Configuration Guide*

Protection switchover technologies

Protection switchover technologies aim at recovering network faults. They back up hardware, link, routing, and service information for switchover in case of network faults, to ensure continuity of network services.

Table 3 Protection switchover technologies

Technology	Introduction	Reference
Ethernet Link Aggregation	Ethernet link aggregation, most often simply called link aggregation, aggregates multiple physical Ethernet links into one logical link to increase link bandwidth beyond the limits of any one single link. This logical link is an aggregate link. It allows for link redundancy because the member physical links can dynamically back up one another.	"Configuring Ethernet ink aggregation" in *Layer 2—LAN Switching Configuration Guide*
Smart Link	Smart Link is a feature developed to address the slow convergence issue with STP. It provides link redundancy as well as fast convergence in a dual uplink network, allowing the backup link to take over quickly when the primary link fails.	"Configuring Smart Link" in *High Availability Configuration Guide*
MSTP	As a Layer 2 management protocol, the Multiple Spanning Tree Protocol (MSTP) eliminates Layer 2 loops by selectively blocking redundant links in a network, and in the mean time, allows for link redundancy.	"Configuring spanning tree" in *Layer 2—LAN Switching Configuration Guide*
RRPP	The Rapid Ring Protection Protocol (RRPP) is a link layer protocol designed for Ethernet rings. RRPP can prevent broadcast storms caused by data loops when an Ethernet ring is healthy, and rapidly restore the communication paths between the nodes in the event that a link is disconnected on the ring.	"Configuring RRPP" in *High Availability Configuration Guide*
FRR (available only on the HP 5500 EI)	Fast Reroute (FRR) provides a quick per-link or per-node protection on an LSP. In this approach, once a link or node fails on a path, FRR comes up to reroute the path to a new link or node to bypass the failed link or node. This can happen as fast as 50 milliseconds minimizing data loss. Protocols such as RIP, OSPF, IS-IS, and static routing support this technology.	*Layer 3—IP Routing Configuration Guide*/Configuration Guide of the corresponding protocols

Technology	Introduction	Reference
GR (available only on the HP 5500 EI)	Graceful Restart (GR) ensures the continuity of packet forwarding when a protocol, such as BGP, IS-IS, OSPF, IPv6 BGP, IPv6 IS-IS, or OSPFv3, restarts or during an active/standby switchover process. It needs other devices to implement routing information backup and recovery.	*Layer 3—IP Routing Configuration Guide*/Configuration Guide of the corresponding protocols
NSR (available only on the HP 5500 EI)	Nonstop Routing (NSR) ensures non-stop data transmission during a master/subordinate switchover by backing up IP forwarding information from the master to the subordinate device in an IRF fabric. Upon a master/subordinate switchover, NSR can complete link state recovery and route re-generation without requiring the cooperation of other devices. Only IS-IS supports this feature.	"Configuring IS-IS" in *Layer 3—IP Routing Configuration Guide*
Stateful Failover (available only on the HP 5500 EI)	Two devices back up the services of each other to ensure that the services on them are consistent. If one device fails, the other device can take over the services by using VRRP or dynamic routing protocols. Because the other device has already backed up the services, service traffic can pass through the other device, avoiding service interruption.	"Configuring stateful failover" in *High Availability Configuration Guide*
VRRP (available only on the HP 5500 EI)	Virtual Router Redundancy Protocol (VRRP) is an error-tolerant protocol that provides highly reliable default links on multicast and broadcast LANs such as Ethernet, avoiding network interruption due to failure of a single link.	"Configuring VRRP" in *High Availability Configuration Guide*

A single availability technology cannot solve all problems. Therefore, a combination of availability technologies, chosen on the basis of detailed analysis of network environments and user requirements, should be used to enhance network availability. For example, access-layer devices should be connected to distribution-layer devices over redundant links, and core-layer devices should be fully meshed. Also, network availability should be considered during planning prior to building a network.

Configuring Ethernet OAM

Ethernet OAM overview

Ethernet Operation, Administration and Maintenance (OAM) is a tool that monitors Layer 2 link status and addresses common link-related issues on the "last mile." You can use it to monitor the status of the point-to-point link between two directly connected devices.

Major functions of Ethernet OAM

Ethernet OAM provides the following functions:

- **Link performance monitoring**—Monitors the performance indices of a link, including packet loss, delay, and jitter, and collects traffic statistics of various types
- **Fault detection and alarm**—Checks the connectivity of a link by sending OAM protocol data units (OAMPDUs) and reports to the network administrators when a link error occurs
- **Remote loopback**—Checks link quality and locates link errors by looping back OAMPDUs

Ethernet OAMPDUs

Ethernet OAM works on the data link layer. Ethernet OAM reports the link status by periodically exchanging OAMPDUs between devices so that the administrator can effectively manage the network.

Ethernet OAMPDUs fall into the following types: Information, Event Notification, and Loopback Control.

Figure 1 Formats of different types of Ethernet OAMPDUs

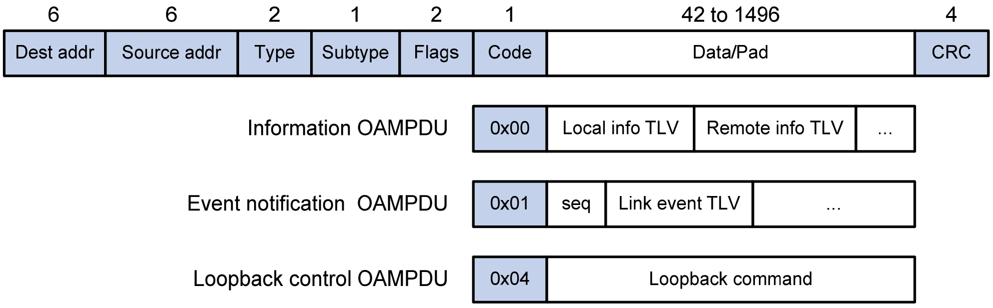


Table 4 Fields in an OAMPDU

Field	Description
Dest addr	Destination MAC address of the Ethernet OAMPDU It is a slow protocol multicast address, 0180c2000002. Bridges cannot forward slow protocol packets, so Ethernet OAMPDUs cannot be forwarded.
Source addr	Source MAC address of the Ethernet OAMPDU It is the bridge MAC address of the sending side and is a unicast MAC address.
Type	Type of the encapsulated protocol in the Ethernet OAMPDU The value is 0x8809.

Field	Description
Subtype	The specific protocol being encapsulated in the Ethernet OAMPDU The value is 0x03.
Flags	Status information of an Ethernet OAM entity
Code	Type of the Ethernet OAMPDU

NOTE:

Throughout this document, a port with Ethernet OAM enabled is an Ethernet OAM entity or an OAM entity.

Table 5 Functions of different types of OAMPDUs

OAMPDU type	Function
Information OAMPDU	Used for transmitting state information of an Ethernet OAM entity—including the information about the local device and remote devices and customized information—to the remote Ethernet OAM entity and maintaining OAM connections.
Event Notification OAMPDU	Used by link monitoring to notify the remote OAM entity when it detects problems on the link in between.
Loopback Control OAMPDU	Used for remote loopback control. By inserting the information used to enable/disable loopback to a loopback control OAMPDU, you can enable/disable loopback on a remote OAM entity.

How Ethernet OAM works

This section describes the working procedures of Ethernet OAM.

Ethernet OAM connection establishment

Ethernet OAM connection is the basis of all the other Ethernet OAM functions. OAM connection establishment is also known as the "Discovery phase", where an Ethernet OAM entity discovers remote OAM entities and establishes sessions with them.

In this phase, interconnected OAM entities determine whether Ethernet OAM connections can be established, by exchanging Information OAMPDUs to notify the peer of their OAM configuration information and the OAM capabilities of the local nodes. An Ethernet OAM connection can be established between entities that have matching Loopback, link detecting, and link event settings. After an Ethernet OAM connection is established, Ethernet OAM takes effect on both sides.

For Ethernet OAM connection establishment, a device can operate in active Ethernet OAM mode or passive Ethernet OAM mode, but a switch role will be somewhat different depending on the mode.

Table 6 Active Ethernet OAM mode and passive Ethernet OAM mode

Item	Active Ethernet OAM mode	Passive Ethernet OAM mode
Initiating OAM Discovery	Available	Unavailable
Responding to OAM Discovery	Available	Available
Transmitting Information OAMPDUs	Available	Available

Item	Active Ethernet OAM mode	Passive Ethernet OAM mode
Transmitting Event Notification OAMPDUs	Available	Available
Transmitting Information OAMPDUs without any TLV	Available	Available
Transmitting Loopback Control OAMPDUs	Available	Unavailable
Responding to Loopback Control OAMPDUs	Available—if both sides operate in active OAM mode	Available

NOTE:

- Only OAM entities operating in active OAM mode can initiate OAM connections. OAM entities operating in passive mode wait and respond to the connection requests sent by their peers.
- No OAM connection can be established between OAM entities operating in passive OAM mode.

After an Ethernet OAM connection is established, the Ethernet OAM entities on both sides exchange Information OAMPDUs at the handshake packet transmission interval to check whether the Ethernet OAM connection is normal. If an Ethernet OAM entity receives no Information OAMPDU within the Ethernet OAM connection timeout time, the Ethernet OAM connection is considered disconnected.

Link monitoring

Error detection in an Ethernet is difficult, especially when the physical connection in the network is not disconnected but network performance is degrading gradually. Link monitoring is used to detect and indicate link faults in various environments. Ethernet OAM implements link monitoring through the exchange of Event Notification OAMPDUs. When detecting one of the link error events listed in Table 7, the local OAM entity sends an Event Notification OAMPDU to notify the remote OAM entity. With the log information, network administrators can keep track of network status promptly.

Table 7 Ethernet OAM link error events

Ethernet OAM link events	Description
Errored symbol event	An errored symbol event occurs when the number of detected symbol errors during a specified detection interval exceeds the predefined threshold.
Errored frame event	An errored frame event occurs when the number of detected error frames during a specified interval exceeds the predefined threshold.
Errored frame period event	An errored frame period event occurs if the number of frame errors in a specific number of received frames exceeds the predefined threshold.
Errored frame seconds event	An errored frame seconds event occurs when the number of error frame seconds detected on a port during a specified detection interval reaches the error threshold.

The system transforms the period of detecting errored frame period events into the maximum number of 64-byte frames (excluding the interframe spacing and preamble) that a port can send in the specified period. The system takes the maximum number of frames sent as the period. The maximum number of frames sent is calculated using this formula: the maximum number of frames = interface bandwidth (bps) × errored frame period event detection period (in ms)/(64 × 8 × 1000).

A second in which errored frames appear is called an "errored frame second."

Remote fault detection

Information OAMPDUs are exchanged periodically among Ethernet OAM entities across established OAM connections. In a network where traffic is interrupted due to device failures or unavailability, the flag field defined in information OAMPDUs allows an Ethernet OAM entity to send error information—the critical link event type—to its peer. You can use the log information to track ongoing link status and troubleshoot problems promptly.

Table 8 Critical link events

Type	Description	OAMPDU transmission frequencies
Link Fault	Peer link signal is lost.	Once per second
Dying Gasp	A power failure or other unexpected error occurred.	Non-stop
Critical Event	An undetermined critical event occurred.	Non-stop

This Switch Series is able to receive information OAMPDUs carrying the critical link events listed in Table 8.

Only the Gigabit fiber ports are able to send information OAMPDUs carrying Link Fault events.

This Switch Series is able to send information OAMPDUs carrying Dying Gasp events when the device is rebooted or relevant ports are manually shut down. Physical IRF ports, however, are unable to send this type of OAMPDU. For more information about physical IRF ports, see *IRF Configuration Guide*.

This Switch Series is unable to send information OAMPDUs carrying Critical Events.

Remote loopback

Remote loopback is available only after the Ethernet OAM connection is established. With remote loopback enabled, the Ethernet OAM entity operating in active Ethernet OAM mode sends non-OAMPDUs to its peer. After receiving these frames, the peer does not forward them according to their destination addresses. Instead, it returns them to the sender along the original path.

Remote loopback enables you to check the link status and locate link failures. Performing remote loopback periodically helps to detect network faults promptly. Furthermore, performing remote loopback by network segments helps to locate network faults.

Standards and protocols

Ethernet OAM is defined in IEEE 802.3ah (Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.

Ethernet OAM configuration task list

Task		Remarks
Configuring basic Ethernet OAM functions		Required
Configuring the Ethernet OAM connection detection timers		Optional
Configuring link monitoring	Configuring errored symbol event detection	Optional
	Configuring errored frame event detection	Optional

Task		Remarks
	Configuring errored frame period event detection	Optional
	Configuring errored frame seconds event detection	Optional
Configuring Ethernet OAM remote loopback	Enabling Ethernet OAM remote loopback	Optional
	Rejecting the Ethernet OAM remote loopback request from a remote port	Optional

Configuring basic Ethernet OAM functions

For Ethernet OAM connection establishment, an Ethernet OAM entity operates in active mode or passive mode. Only an Ethernet OAM entity in active mode can initiate connection establishment. After Ethernet OAM is enabled on an Ethernet port, according to its Ethernet OAM mode, the Ethernet port establishes an Ethernet OAM connection with its peer port.

To change the Ethernet OAM mode on an Ethernet OAM-enabled port, you must first disable Ethernet OAM on the port.

To configure basic Ethernet OAM functions:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Set the Ethernet OAM mode.	**oam mode** { **active** | **passive** }	Optional. The default is active Ethernet OAM mode.
4. Enable Ethernet OAM on the current port.	**oam enable**	Ethernet OAM is disabled by default.

Configuring the Ethernet OAM connection detection timers

After an Ethernet OAM connection is established, the Ethernet OAM entities on both sides exchange Information OAMPDUs at the handshake packet transmission interval to check whether the Ethernet OAM connection is normal. If an Ethernet OAM entity receives no Information OAMPDU within the Ethernet OAM connection timeout time, the Ethernet OAM connection is considered disconnected.

By adjusting the handshake packet transmission interval and the connection timeout timer, you can change the detection time resolution for Ethernet OAM connections.

After the timeout timer of an Ethernet OAM connection expires, the local OAM entity ages out its connection with the peer OAM entity, causing the OAM connection to be disconnected. HP recommends that you set the connection timeout timer to at least five times the handshake packet transmission interval, ensuring the stability of Ethernet OAM connections.

To configure the Ethernet OAM connection detection timers:

Step		Command	Remarks
5.	Enter system view.	**system-view**	N/A
6.	Configure the Ethernet OAM handshake packet transmission interval.	**oam timer hello** *interval*	Optional. 1000 millisecond by default.
7.	Configure the Ethernet OAM connection timeout timer.	**oam timer keepalive** *interval*	Optional. 5000 milliseconds by default.

Configuring link monitoring

After Ethernet OAM connections are established, the link monitoring periods and thresholds configured in this section take effect on all Ethernet ports automatically.

Configuring errored symbol event detection

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Configure the errored symbol event detection interval.	**oam errored-symbol period** *period-value*	Optional. 1 second by default.
3.	Configure the errored symbol event triggering threshold.	**oam errored-symbol threshold** *threshold-value*	Optional. 1 by default.

Configuring errored frame event detection

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Configure the errored frame event detection interval.	**oam errored-frame period** *period-value*	Optional. 1 second by default.
3.	Configure the errored frame event triggering threshold.	**oam errored-frame threshold** *threshold-value*	Optional. 1 by default.

Configuring errored frame period event detection

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Configure the errored frame period event detection period.	**oam errored-frame-period period** *period-value*	Optional. 1000 milliseconds by default.

Step		Command	Remarks
3.	Configure the errored frame period event triggering threshold.	**oam errored-frame-period threshold** *threshold-value*	Optional. 1 by default.

Configuring errored frame seconds event detection

IMPORTANT:

Make sure the errored frame seconds triggering threshold is less than the errored frame seconds detection interval. Otherwise, no errored frame seconds event can be generated.

To configure errored frame seconds event detection:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Configure the errored frame seconds event detection interval.	**oam errored-frame-seconds period** *period-value*	Optional. 60 second by default.
3.	Configure the errored frame seconds event triggering threshold.	**oam errored-frame-seconds threshold** *threshold-value*	Optional. 1 by default.

Configuring Ethernet OAM remote loopback

Enabling Ethernet OAM remote loopback

CAUTION:

Use this function with caution, because enabling Ethernet OAM remote loopback impacts other services.

When you enable Ethernet OAM remote loopback on a port, the port sends Loopback Control OAMPDUs to a remote port, and the remote port enters the loopback state. The port then sends test frames to the remote port. By observing how many of these test frames return, you can calculate the packet loss ratio on the link to evaluate the link performance.

You can enable Ethernet OAM remote loopback on a specific port in user view, system view, or Layer 2 Ethernet interface view. The configuration effects are the same.

Configuration guidelines

- Ethernet OAM remote loopback is available only after the Ethernet OAM connection is established and can be performed only by Ethernet OAM entities operating in active Ethernet OAM mode.
- Remote loopback is available only on full-duplex links that support remote loopback at both ends.
- Ethernet OAM remote loopback must be supported by both the remote port and the sending port.
- Enabling Ethernet OAM remote loopback interrupts data communications. After Ethernet OAM remote loopback is disabled, all the ports involved will shut down and then come up. Ethernet OAM remote loopback can be disabled by any of the following actions: executing the **undo oam enable** command to disable Ethernet OAM; executing the **undo oam loopback interface** or **undo oam**

loopback command to disable Ethernet OAM remote loopback; and Ethernet OAM connection timing out.

- Ethernet OAM remote loopback is only applicable to individual links. It is not applicable to link aggregation member ports or service loopback group member ports. In addition, do not assign ports where Ethernet OAM remote loopback is being performed to link aggregation groups or service loopback groups. For more information about link aggregation groups and service loopback groups, see *Layer 2—LAN Switching Configuration Guide*.
- Enabling internal loopback test on a port in remote loopback test can terminate the remote loopback test. For more information about loopback test, see *Layer 2—LAN Switching Configuration Guide*.

Configuration procedure

To enable Ethernet OAM remote loopback in user view:

Task	Command	Remarks
Enable Ethernet OAM remote loopback on a specific port.	**oam loopback interface** *interface-type interface-number*	Disabled by default.

To enable Ethernet OAM remote loopback in system view:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable Ethernet OAM remote loopback on a specific port.	**oam loopback interface** *interface-type interface-number*	Disabled by default.

To enable Ethernet OAM remote loopback in Layer 2 Ethernet interface view:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable Ethernet OAM remote loopback on the port.	**oam loopback**	Disabled by default.

Rejecting the Ethernet OAM remote loopback request from a remote port

The Ethernet OAM remote loopback function impacts other services. To solve this problem, you can disable a port from being controlled by the Loopback Control OAMPDUs sent by a remote port. The local port then rejects the Ethernet OAM remote loopback request from the remote port.

To reject the Ethernet OAM remote loopback request from a remote port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Reject the Ethernet OAM remote loopback request from a remote port.	**oam loopback reject-request**	By default, a port does not reject the Ethernet OAM remote loopback request from a remote port.

Displaying and maintaining Ethernet OAM configuration

Task	Command	Remarks
Display global Ethernet OAM configuration.	**display oam configuration** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the statistics on critical events after an Ethernet OAM connection is established.	**display oam critical-event** [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the statistics on Ethernet OAM link error events after an Ethernet OAM connection is established.	**display oam link-event** { **local** | **remote** } [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the information about an Ethernet OAM connection.	**display oam** { **local** | **remote** } [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear statistics on Ethernet OAM packets and Ethernet OAM link error events.	**reset oam** [**interface** *interface-type interface-number*]	Available in user view

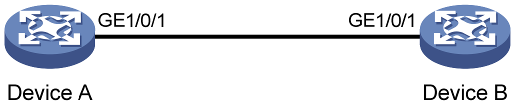
Ethernet OAM configuration example

Network requirements

On the network shown in Figure 2, perform the following operations:

- Enable Ethernet OAM on Device A and Device B to auto-detect link errors between the two devices
- Monitor the performance of the link between Device A and Device B by collecting statistics about the error frames received by Device A

Figure 2 Network diagram



Configuration procedure

1. Configure Device A:

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

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

   # Set the errored frame detection interval to 20 seconds and set the errored frame event triggering threshold to 10.

```
[DeviceA] oam errored-frame period 20
[DeviceA] oam errored-frame threshold 10
```

2. Configure Device B:

   # Configure GigabitEthernet 1/0/1 to operate in active Ethernet OAM mode (the default) and enable Ethernet OAM for it.

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] oam mode active
[DeviceB-GigabitEthernet1/0/1] oam enable
[DeviceB-GigabitEthernet1/0/1] quit
```

3. Verify the configuration:

   Use the **display oam configuration** command to display the Ethernet OAM configuration. For example:

   # Display the Ethernet OAM configuration on Device A.

```
[DeviceA] display oam configuration
Configuration of the link event window/threshold :
--------------------------------------------------------------------------
Errored-symbol Event period(in seconds)           :     1
Errored-symbol Event threshold                    :     1
Errored-frame Event period(in seconds)            :     20
Errored-frame Event threshold                     :     10
Errored-frame-period Event period(in ms)          :     1000
Errored-frame-period Event threshold              :     1
Errored-frame-seconds Event period(in seconds)    :     60
Errored-frame-seconds Event threshold             :     1

Configuration of the timer :
--------------------------------------------------------------------------
Hello timer(in ms)                                :     1000
Keepalive timer(in ms)                            :     5000
```

The output shows that the detection period of errored frame events is 20 seconds, the detection threshold is 10 seconds, and all the other parameters use the default values.

You can use the **display oam critical-event** command to display the statistics of Ethernet OAM critical link events. For example:

# Display the statistics of Ethernet OAM critical link events on all the ports of Device A.

```
[DeviceA] display oam critical-event
Port        : GigabitEthernet1/0/1
Link Status : Up
Event statistic :
-------------------------------------------------------------------------
Link Fault    :0    Dying Gasp    : 0    Critical Event    : 0
```

The output shows that no critical link event occurred on the link between Device A and Device B.

You can use the **display oam link-event** command to display the statistics of Ethernet OAM link error events. For example:

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

```
[DeviceB] display oam link-event remote
Port :GigabitEthernet1/0/1
Link Status :Up
OAMRemoteErrFrameEvent : (ms = milliseconds)
---------------------------------------------------------------------
Event Time Stamp          : 5789        Errored FrameWindow   : 200(100ms)
Errored Frame Threshold   : 10          Errored Frame         : 13
Error Running Total       : 350         Event Running Total   : 17
```

The output shows that 350 errors occurred since Ethernet OAM was enabled on Device A, 17 of which are caused by error frames. The link is unstable.

Configuring CFD

Overview

Connectivity Fault Detection (CFD) is an end-to-end per-VLAN link layer OAM mechanism used for link connectivity detection, fault verification, and fault location. It conforms to IEEE 802.1ag CFM and ITU-T Y.1731.

Basic CFD concepts

This section explains the concepts of CFD.

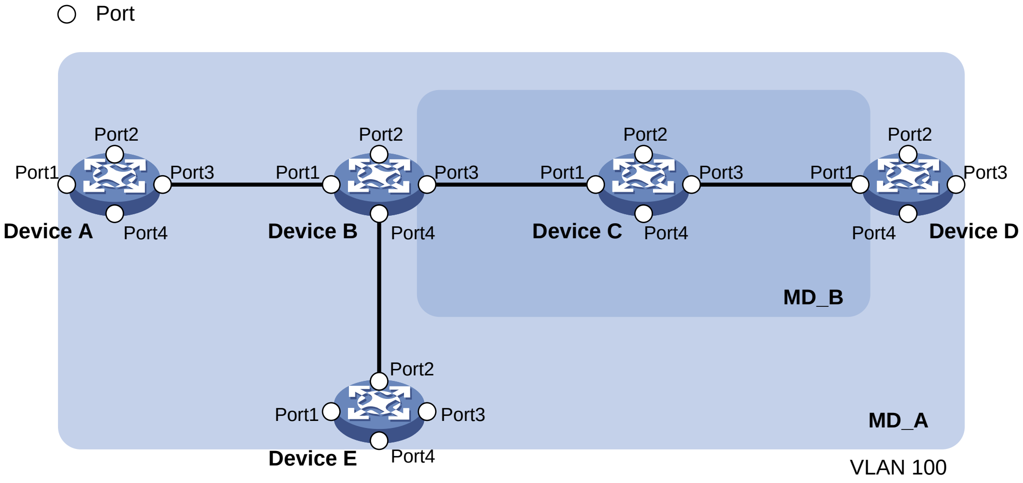
MD

A maintenance domain (MD) defines the network or part of the network where CFD plays its role. An MD is identified by its MD name.

To accurately locate faults, CFD assigns eight levels ranging from 0 to 7 to MDs. The bigger the number, the higher the level, and the larger the area covered. If the outer domain has a higher level than the nested one, domains can touch or nest, but they cannot intersect or overlap.

MD levels facilitate fault location and its accuracy. As shown in Figure 3, MD_A in light blue nests MD_B in dark blue. If a connectivity fault is detected at the boundary of MD_A, any of the devices in MD_A, including Device A through Device E, may fail. If a connectivity fault is also detected at the boundary of MD_B, the failure points may be any of Device B through Device D. If the devices in MD_B can operate properly, at least Device C is operational.

Figure 3 Two nested MDs



CFD exchanges messages and performs operations on a per-domain basis. By planning MDs properly in a network, you can use CFD to rapidly locate failure points.

MA

A maintenance association (MA) is a part of an MD. You can configure multiple MAs in an MD as needed. An MA is identified by the "MD name + MA name".

An MA serves a VLAN. Packets sent by the MPs in an MA carry the relevant VLAN tag. An MP can receive packets sent by other MPs in the same MA. The level of an MA equals the level of the MD that the MA belongs to.

MP

An MP is configured on a port and belongs to an MA. MPs include maintenance association end points (MEPs) and maintenance association intermediate points (MIPs).

- MEPs

  MEPs define the boundary of the MA. Each MEP is identified by a MEP ID.

  The MA to which a MEP belongs defines the VLAN of packets sent by the MEP. The level of a MEP is equal to the level of the MD to which the MEP belongs, and the level of packets sent by a MEP equals the level of the MEP. The level of a MEP determines the levels of packets that the MEP can process. A MEP forwards packets at a higher level and processes packets of its own level or lower. The processing procedure is specific to packets in the same VLAN. Packets of different VLANs are independent.

  MEPs are either inward-facing or outward-facing. An outward-facing MEP sends packets to its host port. An inward-facing MEP does not send packets to its host port. Rather, it sends packets to other ports on the device.

- MIP

  A MIP is internal to an MA. It cannot send CFD packets actively. However, a MIP can handle and respond to CFD packets. By cooperating with MEPs, a MIP can perform a function similar to ping and traceroute. A MIP forwards packets of a different level without any processing and only processes packet of its own level.

  The MA to which a MIP belongs defines the VLAN of packets that the MEP can receive. The level of a MIP is defined by its generation rule and the MD that the MIP belongs to. MIPs are generated on each port automatically according to related MIP generation rules. If a port has no MIP, the system will examine the MAs in each MD (from low to high levels), and follow the procedure as described in Figure 4 to determine whether to create MIPs at the relevant level.

Figure 4 Procedure of creating MIPs

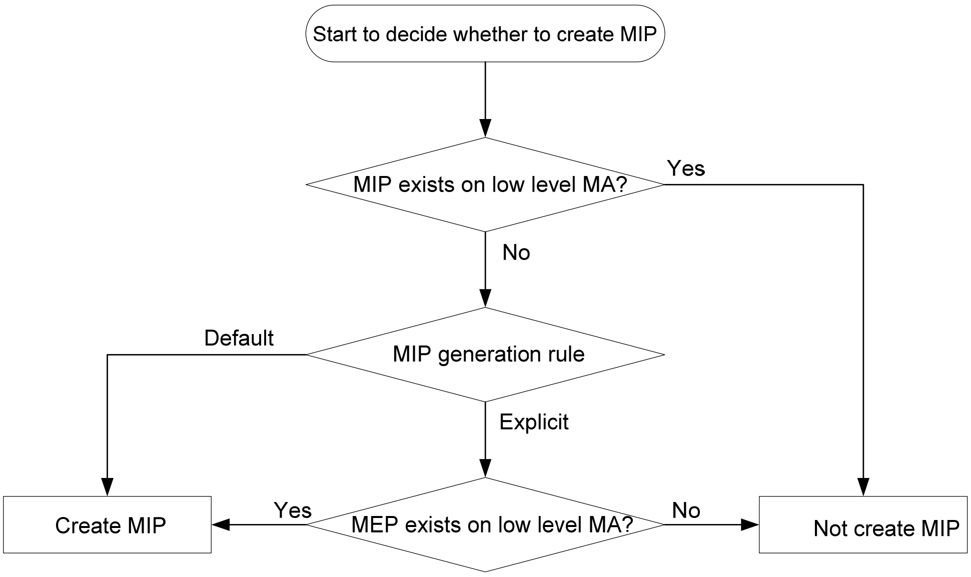
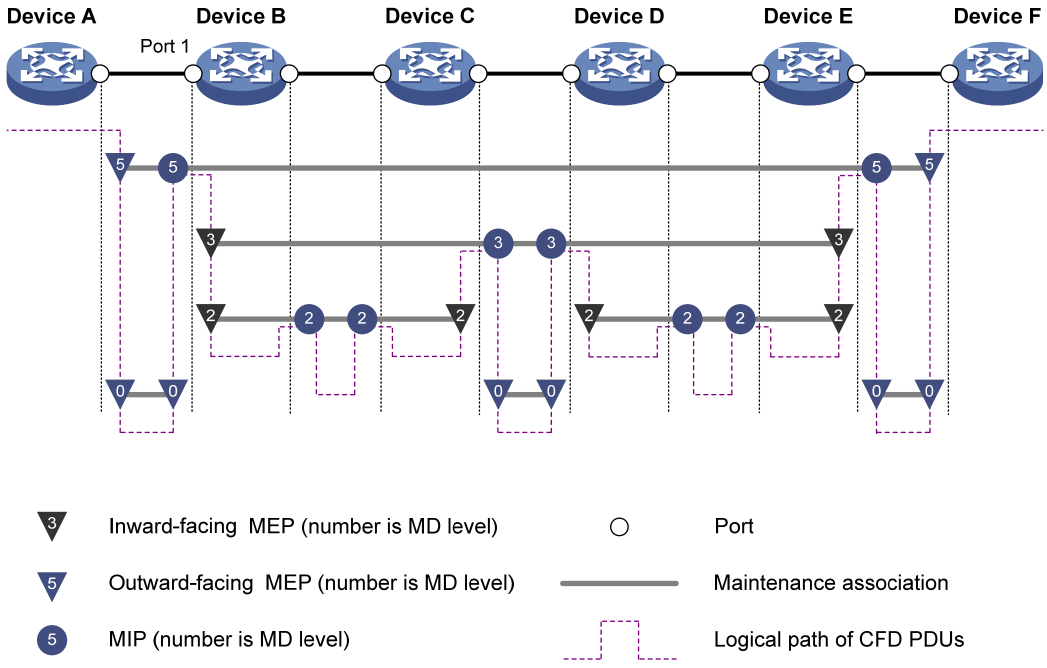

Start to decide whether to create MIP
MIP exists on low level MA?
Yes
No
Default
MIP generation rule
Explicit
Create MIP
Yes
MEP exists on low level MA?
No
Not create MIP

Figure 5 demonstrates a grading example of the CFD module. Four levels of MDs (0, 2, 3, and 5) are designed. The bigger the number, the higher the level, and the larger the area covered. MPs are configured on the ports of device A through device F. Port 1 of device B is configured with the following MPs—a level 5 MIP, a level 3 inward-facing MEP, a level 2 inward-facing MEP, and a level 0 outward-facing MEP.

Figure 5 CFD grading example



MEP list

A MEP list is a collection of configurable local MEPs and the remote MEPs to be monitored in the same MA. It lists all MEPs configured on different devices in the same MA. The MEPs all have unique MEP IDs. When a MEP receives from a remote device a continuity check message (CCM) with a MEP ID not included in the MEP list of the MA, it drops the message.

CFD functions

CFD works effectively only in properly configured networks. Its functions, which are implemented through the MPs, include:

- Continuity check (CC)
- Loopback (LB)
- Linktrace (LT)
- Alarm indication signal (AIS)
- Loss measurement (LM)
- Delay measurement (DM)
- Test (TST)

CC

Connectivity faults are usually caused by device faults or configuration errors. CC examines the connectivity between MEPs. This function is implemented through periodic sending of continuity check messages (CCMs) by the MEPs. A CCM sent by one MEP is intended to be received by all of the other MEPs in the same MA. If a MEP fails to receive the CCMs within 3.5 times the sending interval, the link is considered faulty and a log is generated. When multiple MEPs send CCMs at the same time, the multipoint-to-multipoint link check is achieved. CCM frames are multicast frames.

LB

Similar to ping at the IP layer, LB verifies the connectivity between a source device and a target device. To implement this function, the source MEP sends loopback messages (LBMs) to the target MEP. Depending on whether the source MEP can receive a loopback reply message (LBR) from the target MEP, the link state between the two can be verified. LBM frames and LBR frames are unicast frames.

LT

LT is similar to traceroute. It identifies the path between the source MEP and the target MP. This function is implemented in the following way—the source MEP sends the linktrace messages (LTMs) to the target MP. After receiving the messages, the target MP and the MIPs that the LTM frames pass send back linktrace reply messages (LTRs) to the source MEP. Based on the reply messages, the source MEP can identify the path to the target MP. LTM frames are multicast frames and LTRs are unicast frames.

AIS

The AIS function suppresses the number of error alarms reported by MEPs. If a local MEP receives no CCM frames from its peer MEP within 3.5 times the CCM transmission interval, it immediately starts to send AIS frames periodically in the opposite direction of CCM frames. Upon receiving the AIS frames, the peer MEP suppresses the error alarms locally, and continues to send the AIS frames. If the local MEP receives CCM frames within 3.5 times the CCM transmission interval, it stops sending AIS frames and restores the error alarm function. AIS frames are multicast frames.

LM

The LM function measures the frame loss in a certain direction between a pair of MEPs. The source MEP sends loss measurement messages (LMMs) to the target MEP, the target MEP responds with loss measurement replies (LMRs), and the source MEP calculates the number of lost frames according to the counter values of the two consecutive LMRs (the current LMR and the previous LMR). LMMs and LMRs are multicast frames.

DM

The DM function measures frame delays between two MEPs, including one-way and two-way frame delays.

1. One-way frame delay measurement

   The source MEP sends a one-way delay measurement (1DM) frame, which carries the transmission time, to the target MEP. Upon receiving the 1DM frame, the target MEP records the reception time, and calculates and records the link transmission delay and jitter (delay variation) according to the transmission time and reception time. 1DM frames are multicast frames.

2. Two-way frame delay measurement

   The source MEP sends a delay measurement message (DMM), which carries the transmission time, to the target MEP. Upon receiving the DMM, the target MEP responds with a delay measurement reply (DMR), which carries the reception time and transmission time of the DMM and the transmission time of the DMR. Upon receiving the DMR, the source MEP records the DMR reception time, and calculates the link transmission delay and jitter according to the DMR reception time and DMM transmission time. DMM frames and DMR frames are multicast frames.

TST

The TST function tests the bit errors between two MEPs. The source MEP sends a TST frame, which carries the test pattern, such as pseudo random bit sequence (PRBS) or all-zero, to the target MEP. Upon receiving the TST frame, the target MEP determines the bit errors by calculating and comparing the content of the TST frame. TST frames are unicast frames.

Protocols and standards

- IEEE 802.1ag, *Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management*
- ITU-T Y.1731, *OAM functions and mechanisms for Ethernet based networks*

CFD configuration task list

For CFD to operate properly, design the network by performing the following tasks:

- Grade the MDs in the entire network and define the boundary of each MD.
- Assign a name for each MD. Make sure the same MD has the same name on different devices.
- Define the MA in each MD according to the VLAN you want to monitor.
- Assign a name for each MA. Make sure the same MA in the same MD has the same name on different devices.
- Determine the MEP list of each MA in each MD. Make sure devices in the same MA maintain the same MEP list.
- At the edges of MD and MA, MEPs should be designed at the device port. MIPs can be designed on devices or ports that are not at the edges.

Tasks			Remarks
Configuring basic CFD settings	Enabling CFD		Required.
	Configuring the CFD protocol version		Optional.
	Configuring service instances	Creating a service instance with the MD name	Required. Perform either task.
		Creating a service instance without the MD name	
	Configuring MEPs		Required.
	Configuring MIP generation rules		Required.
Configuring CFD functions	Configuring CC on MEPs		Required.
	Configuring LB on MEPs		Optional.
	Configuring LT on MEPs		Optional.
	Configuring AIS		Optional.
	Configuring LM		Optional.
	Configuring one-way DM		Optional.
	Configuring two-way DM		Optional.
	Configuring TST		Optional.

Typically, a port blocked by the spanning tree feature cannot receive or send CFD messages except in the following cases:

- The port is configured as an outward-facing MEP.

- The port is configured as a MIP or an inward-facing MEP that can still receive and send CFD messages except CCM messages.

For more information about the spanning tree feature, see *Layer 2—LAN Switching Configuration Guide*.

Configuring basic CFD settings

This section provides procedures for configuring basic CFD settings.

Enabling CFD

Enable CFD before you perform other configuration tasks.

To enable CFD on a device:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable CFD.	**cfd enable**	By default, CFD is disabled.

Configuring the CFD protocol version

Three CFD protocol versions are available: IEEE 802.1ag draft5.2 version, IEEE 802.1ag draft5.2 interim version, and IEEE 802.1ag standard version.

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

If an MD is created by using the **cfd md** command or automatically generated by using the **cfd service-instance maid format** command on a device, you cannot switch between the standard version and draft5.2 version (or draft5.2 interim version). However, you can switch between the draft5.2 version and draft5.2 interim version. This restriction does not apply to the device without an MD configured.

To configure the CFD protocol version:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the CFD protocol version.	**cfd version** { **draft5** | **draft5-plus** | **standard** }	Optional. By default, CFD uses the standard version of IEEE 802.1ag.

Configuring service instances

Before configuring the MEPs and MIPs, first configure service instances. A service instance is a set of service access points (SAPs), and belongs to an MA in an MD.

A service instance is indicated by an integer to represent an MA in an MD. The MD and MA define the level and VLAN attribute of the messages handled by the MPs in a service instance.

Service instances fall into two types:

- Service instance with the MD name, which takes effect in any version of CFD.

- Service instance without the MD name, which takes effect in only CFD IEEE 802.1ag.

You can create either type of service instance as needed.

Creating a service instance with the MD name

To create a service instance with the MD name, create the MD and MA for the service instance first.

To configure a service instance with the MD name:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an MD.	**cfd md** *md-name* **level** *level-value*	By default, no MD is created.
3. Create an MA.	**cfd ma** *ma-name* **md** *md-name* **vlan** *vlan-id*	By default, no MA is created.
4. Create a service instance with the MD name	**cfd service-instance** *instance-id* **md** *md-name* **ma** *ma-name*	By default, no service instance with the MD name is created.

Creating a service instance without the MD name

When you create a service instance without the MD name, the system automatically creates the MA and MD for the service instance.

To create a service instance without the MD name:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a service instance without the MD name.	**cfd service-instance** *instance-id* **maid format** { **icc-based** *ma-name* | **string** *ma-name* } **level** *level-value* **vlan** *vlan-id*	By default, no service instance without the MD name is created.

Configuring MEPs

CFD is implemented through various operations on MEPs. A MEP is configured on a service instance, so the MD level and VLAN attribute of the service instance become the attribute of the MEP.

Before creating MEPs, configure the MEP list. A MEP list is a collection of local configurable MEPs in an MA and the remote MEPs to be monitored.

To configure a MEP:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a MEP list.	**cfd meplist** *mep-list* **service-instance** *instance-id*	By default, no MEP list is configured. To create a MEP, the MEP ID must be included in the MEP list of the service instance.
3. Enter Layer 2 Ethernet interface view.	**interface** *interface-type* *interface-number*	N/A

Step	Command	Remarks
4. Create a MEP.	**cfd mep** *mep-id* **service-instance** *instance-id* { **inbound** | **outbound** }	By default, no MEP is created.
5. Enable the MEP.	**cfd mep service-instance** *instance-id* **mep** *mep-id* **enable**	By default, the MEP is disabled.

Configuring MIP generation rules

As functional entities in a service instance, MIPs respond to various CFD frames, such as LTM frames, LBM frames, 1DM frames, DMM frames, and TST frames. You can choose appropriate MIP generation rules based on your network design.

Any of the following actions or cases can cause MIPs to be created or deleted after you configure the **cfd mip-rule** command:

- Enabling or disabling CFD (use the **cfd enable** command).
- Creating or deleting the MEPs on a port.
- Changes occur to the VLAN attribute of a port.
- The rule specified in the **cfd mip-rule** command changes.

To configure the rules for generating MIPs:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the rules for generating MIPs.	**cfd mip-rule** { **default** | **explicit** } **service-instance** *instance-id*	By default, neither MIPs nor the rules for generating MIPs are configured.

Configuring CFD functions

This section provides information about configuring CFD functions.

Configuration prerequisites

Complete basic CFD settings.

Configuring CC on MEPs

This section describes how to configure CC on MEPs.

Configuration guidelines

- Configure CC before you configure other CFD functions. After the CC function is configured, MEPs can send CCM frames to each other to examine the connectivity between them.
- Configure the same interval field value in CCM messages sent by the MEPs belonging to the same MA.

Table 9 Relationship between the interval field value in the CCM message, the interval between CCM messages, and the timeout time of the remote MEP

The interval field value in the CCM message	The interval between CCM messages	The timeout time of the remote MEP
4	1 second	3.5 seconds
5	10 second	35 seconds
6	60 seconds	210 seconds
7	600 seconds	2100 seconds

Configuration procedure

To configure CC on a MEP:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the interval field value in the CCM messages sent by MEPs.	**cfd cc interval** *interval-value* **service-instance** *instance-id*	Optional. By default, the interval field value is 4.
3. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
4. Enable CCM sending on a MEP.	**cfd cc service-instance** *instance-id* **mep** *mep-id* **enable**	By default, CCM sending on a MEP is disabled.

Configuring LB on MEPs

The LB function can verify the link state between the local MEP and the remote MEP or MIP.

To configure LB on a MEP:

Task	Command	Remarks
Enable LB.	**cfd loopback service-instance** *instance-id* **mep** *mep-id* { **target-mep** *target-mep-id* | **target-mac** *mac-address* } [**number** *number*]	By default, LB is disabled. Available in any view.

Configuring LT on MEPs

LT can trace the path between the source and target MEPs, and can also locate link faults by sending LT messages automatically. The two functions are implemented in the following way:

- To implement the first function, the source MEP first sends LTM messages to the target MEP. Based on the LTR messages in response to the LTM messages, the path between the two MEPs can be identified.
- In the latter case, after LT messages automatic sending is enabled, if the source MEP fails to receive the CCM frames from the target MEP within 3.5 times the transmission interval, the link between the two is considered faulty. LTM frames will be sent out with the target MEP as the destination and the

TTL field in the LTM frames set to the maximum value 255. Based on the LTRs that the MIPs return, the fault source can be located.

To configure LT on MEPs:

Step	Command	Remarks
1. Find the path between a source MEP and a target MEP.	**cfd linktrace service-instance** *instance-id* **mep** *mep-id* { **target-mep** *target-mep-id* | **target-mac** *mac-address* } [**ttl** *ttl-value*] [**hw-only**]	Available in any view.
2. Enter system view.	**system-view**	N/A
3. Enable LT messages automatic sending.	**cfd linktrace auto-detection** [**size** *size-value*]	By default, LT messages automatic sending is disabled.

Configuring AIS

The AIS function suppresses the number of error alarms reported by MEPs.

Configuration guidelines

- To have a MEP in the service instance send AIS frames, configure the AIS frame transmission level to be higher than the MD level of the MEP.
- Enable AIS and configure the proper AIS frame transmission level on the target MEP, so the target MEP can suppress the error alarms and send the AIS frame to the MD of a higher level. If you enable AIS but do not configure the proper AIS frame transmission level on the target MEP, the target MEP can suppress the error alarms, but cannot send the AIS frames.

Configuration procedure

To configure AIS:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable AIS.	**cfd ais enable**	By default, AIS is disabled.
3. Configure the AIS frame transmission level.	**cfd ais level** *level-value* **service-instance** *instance-id*	By default, the AIS frame transmission level is not configured.
4. Configure the AIS frame transmission interval.	**cfd ais period** *period-value* **service-instance** *instance-id*	Optional. The default is 1 second.

Configuring LM

The LM function measures frame loss between MEPs, including the number of lost frames, the frame loss ratio, and the average number of lost frames for the source and target MEPs. The LM function takes effect only in CFD IEEE 802.1ag.

To configure LM:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure LM.	**cfd slm service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]	By default, LM is disabled.

Configuring one-way DM

The one-way DM function measures the one-way frame delay between two MEPs, and monitors and manages the link transmission performance.

Configuration guidelines

- The one-way DM function takes effect only in CFD IEEE 802.1ag.
- One-way DM requires that the clocks at the transmitting MEP and the receiving MEP be synchronized. For the purpose of frame delay variation measurement, the requirement for clock synchronization can be relaxed.
- To view the test result, use the **display cfd dm one-way history** command on the target MEP.

Configuration procedure

To configure one-way DM:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure one-way DM.	**cfd dm one-way service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]	By default, one-way DM is disabled.

Configuring two-way DM

The two-way DM function measures the two-way frame delay, average two-way frame delay, and two-way frame delay variation between two MEPs, and monitors and manages the link transmission performance. The two-way DM function is available only under the IEEE 802.1ag standard version of CFD.

To configure two-way DM:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure two-way DM.	**cfd dm two-way service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]	By default, two-way DM is disabled.

Configuring TST

The TST function detects bit errors on a link, and monitors and manages the link transmission performance. The TST function takes effect only in CFD IEEE 802.1ag.

To configure TST:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure TST.	**cfd tst service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*] [**length-of-test** *length*] [**pattern-of-test** { **all-zero** | **prbs** } [**with-crc**]]	By default, TST is disabled. To view the test result, use the **display cfd tst** command on the target MEP.

Displaying and maintaining CFD

Task	Command	Remarks
Display CFD and AIS status.	**display cfd status** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the CFD protocol version.	**display cfd version** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display MD configuration information.	**display cfd md** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display MA configuration information.	**display cfd ma** [[*ma-name*] **md** { *md-name* | **level** *level-value* }] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display service instance configuration information.	**display cfd service-instance** [*instance-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display MEP list in a service instance.	**display cfd meplist** [**service-instance** *instance-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display MP information.	**display cfd mp** [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the attribute and running information of the MEPs.	**display cfd mep** *mep-id* **service-instance** *instance-id* [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Task	Command	Remarks
Display LTR information received by a MEP.	**display cfd linktrace-reply** [**service-instance** *instance-id* [**mep** *mep-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the information of a remote MEP.	**display cfd remote-mep service-instance** *instance-id* **mep** *mep-id* [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the content of the LTR messages received as responses to the automatically sent LTMs.	**display cfd linktrace-reply auto-detection** [**size** *size-value*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the AIS configuration and information on the specified MEP.	**display cfd ais** [**service-instance** *instance-id* [**mep** *mep-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the one-way DM result on the specified MEP.	**display cfd dm one-way history** [**service-instance** *instance-id* [**mep** *mep-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the TST result on the specified MEP.	**display cfd tst** [**service-instance** *instance-id* [**mep** *mep-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear the one-way DM result on the specified MEP.	**reset cfd dm one-way history** [**service-instance** *instance-id* [**mep** *mep-id*]]	Available in user view
Clear the TST result on the specified MEP.	**reset cfd tst** [**service-instance** *instance-id* [**mep** *mep-id*]]	Available in user view

CFD configuration example

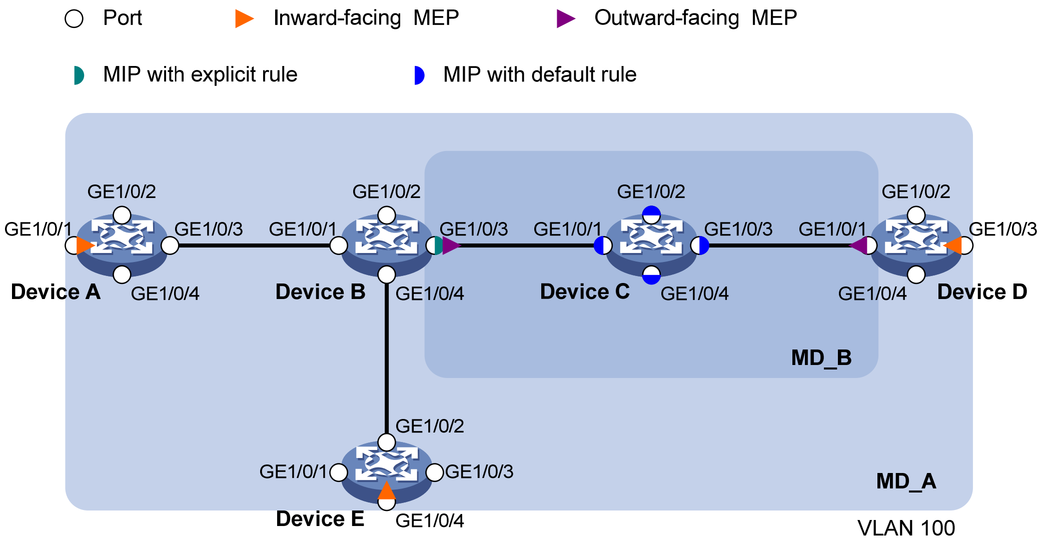
Network requirements

As shown in Figure 6:

- The network comprises five devices and is divided into two MDs: MD_A (level 5) and MD_B (level 3). All ports belong to VLAN 100, and the MAs in the two MDs all serve VLAN 100. Assume that the MAC addresses of Device A through Device E are 0010-FC00-6511, 0010-FC00-6512, 0010-FC00-6513, 0010-FC00-6514, and 0010-FC00-6515, respectively.
- MD_A has three edge ports: GigabitEthernet 1/0/1 on Device A, GigabitEthernet 1/0/3 on Device D, and GigabitEthernet 1/0/4 on Device E. They are all inward-facing MEPs. MD_B has two edge ports: GigabitEthernet 1/0/3 on Device B and GigabitEthernet 1/0/1 on Device D. They are both outward-facing MEPs.
- In MD_A, Device B is designed to have MIPs when its port is configured with low-level MEPs. Port GigabitEthernet 1/0/3 is configured with MEPs of MD_B, and the MIPs of MD_A can be configured on this port. Configure the MIP generation rule of MD_A as explicit.

- The MIPs of MD_B are designed on Device C, and are configured on all ports. You should configure the MIP generation rule as default.
- Configure CC to monitor the connectivity among all the MEPs in MD_A and MD_B. Configure LB to locate link faults, and use the AIS function to suppress the error alarms reported.
- After the status information of the entire network is obtained, use LT, LM, one-way DM, two-way DM, and TST to detect link faults.

Figure 6 Network diagram



Configuration procedure

1. Configure a VLAN and assign ports to it:

   On each device shown in Figure 6, create VLAN 100 and assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to VLAN 100.

2. Enable CFD:

   # Enable CFD on Device A.

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

   Enable CFD on Device B through Device E using the same method.

3. Configure service instances:

   # Create MD_A (level 5) on Device A, create MA_A, which serves VLAN 100, in MD_A, and create service instance 1 for MD_A and MA_A.

```
[DeviceA] cfd md MD_A level 5
[DeviceA] cfd ma MA_A md MD_A vlan 100
[DeviceA] cfd service-instance 1 md MD_A ma MA_A
```

   Configure Device E as you configure Device A.

   # Create MD_A (level 5) on Device B, create MA_A that serves VLAN 100, in MD_A, and then create service instance 1 for MD_A and MA_A. In addition, create MD_B (level 3) and MA_B that serves VLAN 100, in MD_B, and then create service instance 2 for MD_B and MA_B.

```
[DeviceB] cfd md MD_A level 5
[DeviceB] cfd ma MA_A md MD_A vlan 100
[DeviceB] cfd service-instance 1 md MD_A ma MA_A
```

```
[DeviceB] cfd md MD_B level 3
[DeviceB] cfd ma MA_B md MD_B vlan 100
[DeviceB] cfd service-instance 2 md MD_B ma MA_B
```

Configure Device D in the same way as Device B.

# Create MD_B (level 3) on Device C, create MA_B that serves VLAN 100, in MD_B, and then create service instance 2 for MD_B and MA_B.

```
[DeviceC] cfd md MD_B level 3
[DeviceC] cfd ma MA_B md MD_B vlan 100
[DeviceC] cfd service-instance 2 md MD_B ma MA_B
```

4. Configure MEPs:

# On Device A, configure a MEP list in service instance 1. Create and enable inward-facing MEP 1001 in service instance 1 on GigabitEthernet 1/0/1.

```
[DeviceA] cfd meplist 1001 4002 5001 service-instance 1
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 inbound
[DeviceA-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

# On Device B, configure a MEP list in service instances 1 and 2 respectively. Create and enable outward-facing MEP 2001 in service instance 2 on GigabitEthernet 1/0/3.

```
[DeviceB] cfd meplist 1001 4002 5001 service-instance 1
[DeviceB] cfd meplist 2001 4001 service-instance 2
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] cfd mep 2001 service-instance 2 outbound
[DeviceB-GigabitEthernet1/0/3] cfd mep service-instance 2 mep 2001 enable
[DeviceB-GigabitEthernet1/0/3] quit
```

# On Device D, configure a MEP list in service instances 1 and 2 respectively, create and enable outward-facing MEP 4001 in service instance 2 on GigabitEthernet 1/0/1, and then create and enable inward-facing MEP 4002 in service instance 1 on GigabitEthernet 1/0/3.

```
[DeviceD] cfd meplist 1001 4002 5001 service-instance 1
[DeviceD] cfd meplist 2001 4001 service-instance 2
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd mep 4001 service-instance 2 outbound
[DeviceD-GigabitEthernet1/0/1] cfd mep service-instance 2 mep 4001 enable
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] cfd mep 4002 service-instance 1 inbound
[DeviceD-GigabitEthernet1/0/3] cfd mep service-instance 1 mep 4002 enable
[DeviceD-GigabitEthernet1/0/3] quit
```

# On Device E, configure a MEP list in service instance 1. Create and enable inward-facing MEP 5001 in service instance 1 on GigabitEthernet 1/0/4.

```
[DeviceE] cfd meplist 1001 4002 5001 service-instance 1
[DeviceE] interface gigabitethernet 1/0/4
[DeviceE-GigabitEthernet1/0/4] cfd mep 5001 service-instance 1 inbound
[DeviceE-GigabitEthernet1/0/4] cfd mep service-instance 1 mep 5001 enable
[DeviceE-GigabitEthernet1/0/4] quit
```

5. Configure MIP generation rules:

# Configure the MIP generation rule in service instance 1 on Device B as explicit.

```
[DeviceB] cfd mip-rule explicit service-instance 1
```

# Configure the MIP generation rule in service instance 2 on Device C as default.

```
[DeviceC] cfd mip-rule default service-instance 2
```

6. Configure CC:

   # On Device A, enable the sending of CCM frames for MEP 1001 in service instance 1 on GigabitEthernet 1/0/1.

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

   # On Device B, enable the sending of CCM frames for MEP 2001 in service instance 2 on GigabitEthernet 1/0/3.

   ```
   [DeviceB] interface gigabitethernet 1/0/3
   [DeviceB-GigabitEthernet1/0/3] cfd cc service-instance 2 mep 2001 enable
   [DeviceB-GigabitEthernet1/0/3] quit
   ```

   # On Device D, enable the sending of CCM frames for MEP 4001 in service instance 2 on GigabitEthernet 1/0/1. Enable the sending of CCM frames for MEP 4002 in service instance 1 on GigabitEthernet 1/0/3.

   ```
   [DeviceD] interface gigabitethernet 1/0/1
   [DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 2 mep 4001 enable
   [DeviceD-GigabitEthernet1/0/1] quit
   [DeviceD] interface gigabitethernet 1/0/3
   [DeviceD-GigabitEthernet1/0/3] cfd cc service-instance 1 mep 4002 enable
   [DeviceD-GigabitEthernet1/0/3] quit
   ```

   # On Device E, enable the sending of CCM frames for MEP 5001 in service instance 1 on GigabitEthernet 1/0/4.

   ```
   [DeviceE] interface gigabitethernet 1/0/4
   [DeviceE-GigabitEthernet1/0/4] cfd cc service-instance 1 mep 5001 enable
   [DeviceE-GigabitEthernet1/0/4] quit
   ```

7. Configure AIS:

   # Enable AIS on Device B, and configure the AIS frame transmission level as 2 and AIS frame transmission interval as 1 second in service instance 2.

   ```
   [DeviceB] cfd ais enable
   [DeviceB] cfd ais level 5 service-instance 2
   [DeviceB] cfd ais period 1 service-instance 2
   ```

Verifying the configuration

1. Verify the LB function:

   When the CC function detects a link fault, use the LB function to locate the fault.

   # Enable LB on Device A to examine the status of the link between MEP 1001 and MEP 5001 in service instance 1.

   ```
   [DeviceA] cfd loopback service-instance 1 mep 1001 target-mep 5001
   Loopback to 0010-FC00-6515 with the sequence number start from 1001-43404:
   Reply from 0010-FC00-6515: sequence number=1001-43404 time=5ms
   Reply from 0010-FC00-6515: sequence number=1001-43405 time=5ms
   Reply from 0010-FC00-6515: sequence number=1001-43406 time=5ms
   Reply from 0010-FC00-6515: sequence number=1001-43407 time=5ms
   Reply from 0010-FC00-6515: sequence number=1001-43408 time=5ms
   ```

```
Send:5        Received:5        Lost:0
```

After the whole network status is obtained with the CC function, use the LT function to identify the paths between source and target MEPs and to locate faults.

2. Verify the LT function:

# Identify the path between MEP 1001 and MEP 5001 in service instance 1 on Device A.

```
[DeviceA] cfd linktrace service-instance 1 mep 1001 target-mep 5001
Linktrace to MEP 5001 with the sequence number 1001-43462
MAC Address               TTL     Last MAC         Relay Action
0010-FC00-6515            63      0010-FC00-6512   Hit
```

3. Verify the LM function:

After the CC function obtains the status information of the entire network, use the LM function to test the link status. For example:

# Test the frame loss from MEP 1001 to MEP 4002 in service instance 1 on Device A.

```
[DeviceA] cfd slm service-instance 1 mep 1001 target-mep 4002
Reply from 0010-FC00-6514
Far-end frame loss: 10    Near-end frame loss: 20
Reply from 0010-FC00-6514
Far-end frame loss: 40    Near-end frame loss: 40
Reply from 0010-FC00-6514
Far-end frame loss: 0     Near-end frame loss: 10
Reply from 0010-FC00-6514
Far-end frame loss: 30    Near-end frame loss: 30

Average
Far-end frame loss: 20    Near-end frame loss: 25
Far-end frame loss rate: 25%    Near-end frame loss rate: 32%
Send LMMs: 5        Received: 5        Lost: 0
```

4. Verify the one-way DM function:

After the CC function obtains the status information of the entire network, use the one-way DM function to test the one-way frame delay of a link. For example:

# Test the one-way frame delay from MEP 1001 to MEP 4002 in service instance 1 on Device A.

```
[DeviceA] cfd dm one-way service-instance 1 mep 1001 target-mep 4002
Info: 5 1DM frames process is done, please check the result on the remote device.
```

# Display the one-way DM result on MEP 4002 in service instance 1 on Device D.

```
[DeviceD] display cfd dm one-way history service-instance 1 mep 4002
Service instance: 1
MEP ID: 4002
Send 1DM total number: 0
Received 1DM total number: 5
Frame delay: 10ms  9ms  11ms  5ms  5ms
Delay average: 8ms
Delay variation: 5ms  4ms  6ms  0ms  0ms
Variation average: 3ms
```

5. Verify the two-way DM function:

After the CC function obtains the status information of the entire network, use the two-way DM function to test the two-way frame delay of a link. For example:

# Test the two-way frame delay from MEP 1001 to MEP 4002 in service instance 1 on Device A.

```
[DeviceA] cfd dm two-way service-instance 1 mep 1001 target-mep 4002
Frame delay:
Reply from 0010-FC00-6514: 10ms
Reply from 0010-FC00-6514: 9ms
Reply from 0010-FC00-6514: 11ms
Reply from 0010-FC00-6514: 5ms
Reply from 0010-FC00-6514: 5ms
Average: 8ms
Send DMM frames: 5       Received: 5        Lost: 0

Frame delay variation: 5ms  4ms  6ms  0ms  0ms
Average: 3ms
```

6. Verify the TST function:

   After the CC function obtains the status information of the entire network, use the TST function to test the bit errors of a link. For example:

   # Test the bit errors on the link from MEP 1001 to MEP 4002 in service instance 1 on Device A.

```
[DeviceA] cfd tst service-instance 1 mep 1001 target-mep 4002
Info: TST process is done. Please check the result on the remote device.
```

   # Display the TST result on MEP 4002 in service instance 1 on Device D.

```
[DeviceD] display cfd tst service-instance 1 mep 4002
Service instance: 1
MEP ID: 4002
Send TST total number: 0
Received TST total number: 5
Received from 0010-FC00-6511, sequence number 1: Bit True
Received from 0010-FC00-6511, sequence number 2: Bit True
Received from 0010-FC00-6511, sequence number 3: Bit True
Received from 0010-FC00-6511, sequence number 4: Bit True
Received from 0010-FC00-6511, sequence number 5: Bit True
```

Configuring DLDP

DLDP overview

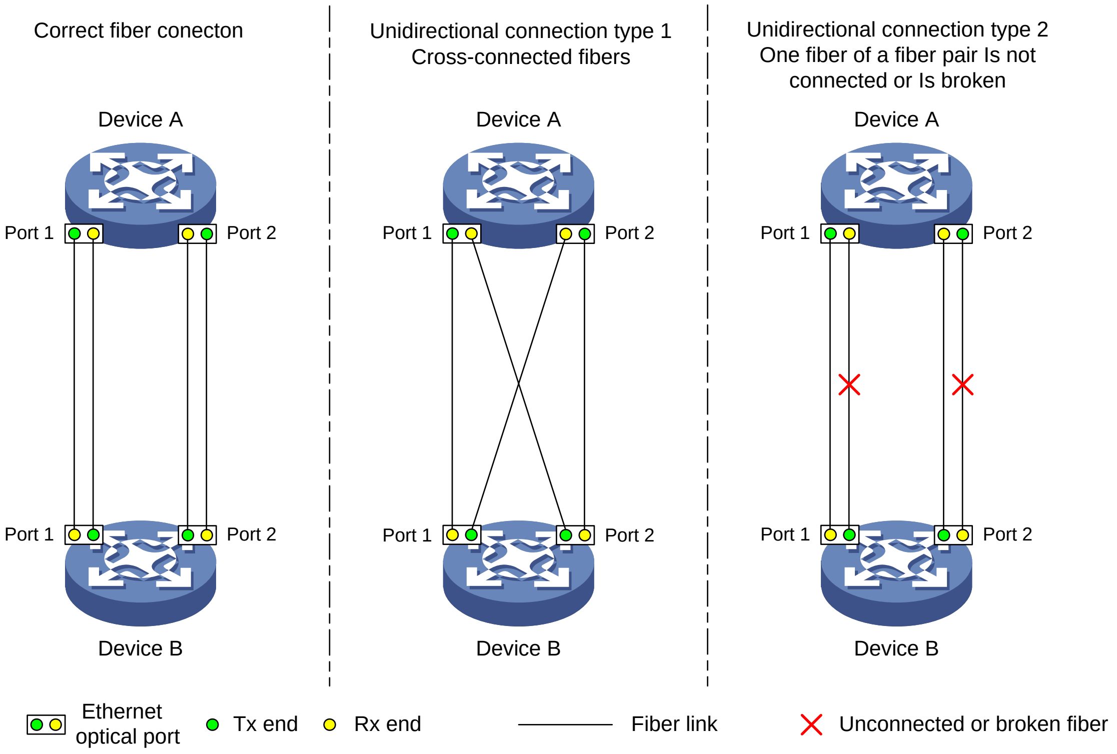
Background

Unidirectional links occur when one end of a link can receive packets from the other end, but the other end cannot receive packets sent by the first end. Unidirectional links result in problems such as loops in an STP-enabled network.

For example, the link between two switches, Switch A and Switch B, is a bidirectional link when they are connected via a fiber pair, with one fiber used for sending packets from A to B and the other for sending packets from B to A. This link is a two-way link. If one of the fibers gets broken, the link becomes a unidirectional link (one-way link).

There are two types of unidirectional fiber links. One occurs when fibers are cross-connected. The other occurs when a fiber is not connected at one end, or when one fiber of a fiber pair gets broken. Figure 7 shows a correct fiber connection and the two types of unidirectional fiber connection.

Figure 7 Correct and incorrect fiber connections



The Device link detection protocol (DLDP) detects unidirectional links (fiber links or twisted-pair links) and can be configured to shut down the related port automatically or prompt users to take actions to avoid network problems.

As a data link layer protocol, DLDP cooperates with physical layer protocols to monitor link status. When the auto-negotiation mechanism provided by the physical layer detects physical signals and faults, DLDP performs operations such as identifying peer devices, detecting unidirectional links, and shutting down unreachable ports. The auto-negotiation mechanism and DLDP work together to make sure that physical/logical unidirectional links are detected and shut down, and to prevent failure of other protocols such as STP. If both ends of a link are operating normally at the physical layer, DLDP detects whether the link is correctly connected at the link layer and whether the two ends can exchange packets properly. This is beyond the capability of the auto-negotiation mechanism at the physical layer.

How DLDP works

DLDP link states

A device is in one of these DLDP link states: Initial, Inactive, Active, Advertisement, Probe, Disable, and DelayDown, as described in Table 10.

Table 10 DLDP link states

State	Description
Initial	DLDP is disabled.
Inactive	DLDP is enabled, and the link is down.
Active	DLDP is enabled and the link is up, or the neighbor entries have been cleared.
Advertisement	All neighbors are bi-directionally reachable or DLDP has been in active state for more than five seconds. This is a relatively stable state where no unidirectional link has been detected.
Probe	DLDP enters this state if it receives a packet from an unknown neighbor. In this state, DLDP sends packets to check whether the link is unidirectional. As soon as DLDP transits to this state, a probe timer starts and an echo timeout timer starts for each neighbor to be probed.
Disable	A port enters this state when: • A unidirectional link is detected. • The contact with the neighbor in enhanced mode gets lost. • In this state, the port does not receive or send packets other than DLDPDUs.
DelayDown	A port in the Active, Advertisement, or Probe DLDP link state transits to this state rather than removes the corresponding neighbor entry and transits to the Inactive state when it detects a port-down event. When a port transits to this state, the DelayDown timer is triggered.

DLDP timers

Table 11 DLDP timers

DLDP timer	Description
Active timer	Determines the interval for sending Advertisement packets with RSY tags, which defaults to 1 second. By default, a device in the active DLDP link state sends one Advertisement packet with RSY tags every second. The maximum number of advertisement packets with RSY tags that can be sent successively is 5.
Advertisement timer	Determines the interval for sending common advertisement packets, which defaults to 5 seconds.
Probe timer	Determines the interval for sending Probe packets, which defaults to 1 second. By default, a device in the probe state sends one Probe packet every second. The maximum number of Probe packets that can be sent successively is 10.

DLDP timer	Description
Echo timer	This timer is set to 10 seconds. It is triggered when a device transits to the Probe state or when an enhanced detect is launched. When the Echo timer expires and no Echo packet has been received from a neighbor device, the state of the link is set to unidirectional and the device transits to the Disable state. In this case, the device does the following: Sends Disable packets. Either prompts the user to shut down the port or shuts down the port automatically (depending on the DLDP down mode configured). Removes the corresponding neighbor entries.
Entry timer	When a new neighbor joins, a neighbor entry is created and the corresponding entry timer is triggered. When a DLDP packet is received, the device updates the corresponding neighbor entry and the entry timer. In normal mode, if no packet is received from a neighbor when the corresponding entry timer expires, DLDP sends advertisement packets with RSY tags and removes the neighbor entry. In enhanced mode, if no packet is received from a neighbor when the Entry timer expires, DLDP triggers the enhanced timer. The setting of an Entry timer is three times that of the Advertisement timer.
Enhanced timer	In enhanced mode, this timer is triggered if no packet is received from a neighbor when the entry timer expires. Enhanced timer is set to 1 second. After the Enhanced timer is triggered, the device sends up to eight probe packets to the neighbor at a frequency of one packet per second.
DelayDown timer	A device in Active, Advertisement, or Probe DLDP link state transits to DelayDown state rather than removes the corresponding neighbor entry and transits to the Inactive state when it detects a port-down event. When a device transits to this state, the DelayDown timer is triggered. A device in DelayDown state only responds to port-up events. If a device in the DelayDown state detects a port-up event before the DelayDown timer expires, it resumes its original DLDP state. If not, when the DelayDown timer expires, the device removes the corresponding DLDP neighbor information and transits to the Inactive state.
RecoverProbe timer	This timer is set to 2 seconds. A port in the Disable state sends one RecoverProbe packet every two seconds to detect whether a unidirectional link has restored.

DLDP mode

DLDP can operate in normal or enhanced mode:

- In normal DLDP mode, when an entry timer expires, the device removes the corresponding neighbor entry and sends an Advertisement packet with the RSY tag.
- In enhanced DLDP mode, when an entry timer expires, the Enhanced timer is triggered and the device tests the neighbor by sending up to eight Probe packets at the frequency of one packet per second. If no Echo packet has been received from the neighbor when the Echo timer expires, the device transits to the Disable state.

Table 12 shows the relationship between the DLDP modes and neighbor entry aging.

Table 12 DLDP mode and neighbor entry aging

DLDP mode	Detecting a neighbor after the corresponding neighbor entry ages out	Removing the neighbor entry immediately after the Entry timer expires	Triggering the Enhanced timer after an Entry timer expires
Normal DLDP mode	No	Yes	No
Enhanced DLDP mode	Yes	No	Yes

Table 13 shows the relationship between DLDP modes and unidirectional link types.

Table 13 DLDP mode and unidirectional link types

Unidirectional link type	Whether it occurs on fibers	Whether it occurs on copper twisted pairs	In which DLDP mode unidirectional links can be detected
Cross-connected link	Yes	No	Both normal and enhanced modes.
Connectionless or broken link	Yes	Yes	Only enhanced mode. The port that can receive signals is in Disable state, and the port that does not receive signals is in Inactive state.

Enhanced DLDP mode is designed for addressing black holes. It prevents situations where one end of a link is up and the other is down.

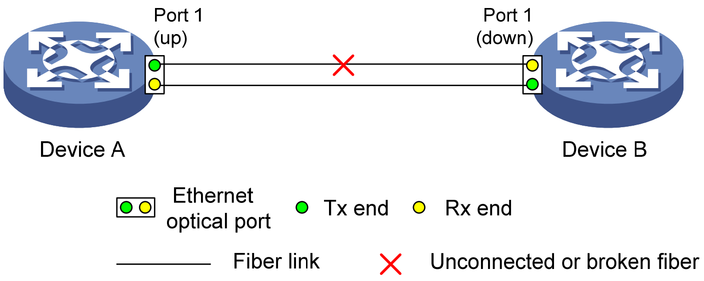
If you configure forced speed and full duplex mode on a port, the situation shown in Figure 8 may occur (take the fiber link for example). Without DLDP enabled, the port on Device B is actually down but its state cannot be detected by common data link protocols, so the port on Device A is still up. However, in enhanced DLDP mode, the following occurs:

The port on Device B is in Inactive DLDP state because it is physically down.

The port on Device A tests the peer port on Device B after the Entry timer for the port on Device B expires.

The port on Device A transits to the Disable state if it does not receive an Echo packet from the port on Device B when the Echo timer expires.

Figure 8 A scenario for the enhanced DLDP mode



DLDP authentication mode

You can use DLDP authentication to prevent network attacks and illegal detection. There are three DLDP authentication modes.

- Non-authentication:
    - The sending side sets the Authentication field and the Authentication type field of DLDP packets to 0.
    - The receiving side checks the values of the two fields of received DLDP packets and drops the packets where the two fields conflict with the corresponding local configuration.
- Simple authentication:
    - Before sending a DLDP packet, the sending side sets the Authentication field to the user-configured password and sets the Authentication type field to 1.
    - The receiving side checks the values of the two fields in received DLDP packets and drops any packets where the two fields conflict with the corresponding local configuration.
- MD5 authentication:
    - Before sending a packet, the sending side encrypts the user configured password using MD5 algorithm, assigns the digest to the Authentication field, and sets the Authentication type field to 2.
    - The receiving side checks the values of the two fields in received DLDP packets and drops any packets where the two fields conflicting with the corresponding local configuration.

DLDP processes

1. On a DLDP-enabled link that is in up state, DLDP sends DLDP packets to the peer device and processes the DLDP packets received from the peer device. DLDP packets sent vary with DLDP states.

Table 14 DLDP packet types and DLDP states

DLDP state	Type of DLDP packets sent
Active	Advertisement packet with RSY tag
Advertisement	Normal Advertisement packet
Probe	Probe packet
Disable	Disable packet and then RecoverProbe packet

NOTE:

A device sends Flush packets when it transits to the Initial state from the Active, Advertisement, Probe, or DelayDown state but does not send them when it transits to the Initial state from Inactive or Disable state.

2. A received DLDP packet is processed with the following methods:
    - In any of the three authentication modes, the packet is dropped if it fails to pass the authentication.
    - The packet is dropped if the setting of the interval to send Advertisement packets it carries conflicts with the corresponding local setting.
    - Other processes are as shown in Table 15.

Table 15 Procedures for processing different types of DLDP packets received

Packet type	Processing procedure	
Advertisement packet with RSY tag	Retrieves the neighbor information	If the corresponding neighbor entry does not exist, creates the neighbor entry, triggers the Entry timer, and transits to Probe state.

Packet type	Processing procedure		
		If the corresponding neighbor entry already exists, resets the Entry timer and transits to Probe state.	
Normal Advertisement packet	Retrieves the neighbor information	If the corresponding neighbor entry does not exist, creates the neighbor entry, triggers the Entry timer, and transits to Probe state.	
		If the corresponding neighbor entry already exists, resets the Entry timer.	
Flush packet	Determines whether or not the local port is in Disable state	If yes, performs no processing.	
		If no, removes the corresponding neighbor entry (if any).	
Probe packet	Retrieves the neighbor information	If the corresponding neighbor entry does not exist, creates the neighbor entry, transits to Probe state, and returns Echo packets.	
		If the corresponding neighbor entry already exists, resets the Entry timer and returns Echo packets.	
Echo packet	Retrieves the neighbor information	If the corresponding neighbor entry does not exist, creates the neighbor entry, triggers the Entry timer, and transits to Probe state.	
		The corresponding neighbor entry already exists	If the neighbor information it carries conflicts with the corresponding locally maintained neighbor entry, drops the packet.
			Otherwise, sets the flag of the neighbor as two-way connected. In addition, if the flags of all the neighbors are two-way connected, the device transits from Probe state to Advertisement state and disables the Echo timer.
Disable packet	Checks whether the local port is in Disable state	If yes, performs no processing.	
		If not, sets the state of the corresponding neighbor to unidirectional, and then checks the state of other neighbors. If all the neighbors are unidirectional, transitions the local port to the Disable state. If the state of some neighbors is unknown, waits until the state of these neighbors is determined. If bidirectional neighbors are present, removes all unidirectional neighbors.	
RecoverProbe packet	Checks whether the local port is in Disable or Advertisement state	If not, performs no processing.	
		If yes, returns RecoverEcho packets.	
RecoverEcho packet	Checks whether the local port is in Disable state	If not, performs no processing.	
		If yes, the local port transits to Active state if the neighbor information the packet carries is consistent with the local port information.	
LinkDown packet	Checks whether the	If not, performs no processing.	

Packet type	Processing procedure	
	local port operates in Enhanced mode	If yes and the local port is not in Disable state, sets the state of the corresponding neighbor to unidirectional, and then checks the state of other neighbors. If all the neighbors are unidirectional, transitions the local port to the Disable state. If the state of some neighbors is unknown, waits until the state of these neighbors is determined. If bidirectional neighbors are present, removes all unidirectional neighbors.

3. If no echo packet is received from the neighbor, DLDP performs the following processing.

Table 16 DLDP process when no echo packet is received from the neighbor

No echo packet received from the neighbor	Processing procedure
In normal mode, no echo packet is received when the Echo timer expires.	DLDP sets the state of the corresponding neighbor to unidirectional, and then checks the state of other neighbors: • If all the neighbors are unidirectional, removes all the neighbors, transitions to the Disable state, outputs log and tracking information, and sends Disable packets. In addition, depending on the user-defined DLDP down mode, shuts down the local port or prompts users to shut down the port. • If the state of some neighbors is unknown, waits until the state of these neighbors is determined. • If bidirectional neighbors are present, removes all unidirectional neighbors.
In enhanced mode, no echo packet is received when the Echo timer expires.	

Link auto-recovery mechanism

If the port shutdown mode upon detection of a unidirectional link is set to **auto**, DLDP automatically sets the state of the port, where a unidirectional link is detected, to DLDP down. A DLDP down port cannot forward data traffic or send/receive any PDUs except DLDPDUs.

On a DLDP down port, DLDP monitors the unidirectional link. Once DLDP finds out that the state of the link has restored to bidirectional, it brings up the port. The specific process is:

The DLDP down port sends out a RecoverProbe packet, which carries only information about the local port, every two seconds. Upon receiving the RecoverProbe packet, the remote end returns a RecoverEcho packet. Upon receiving the RecoverEcho packet, the local port checks whether neighbor information in the RecoverEcho packet is the same as the local port information. If they are the same, the link between the local port and the neighbor is considered to have been restored to a bidirectional link, and the port will transit from Disable state to Active state and re-establish relationship with the neighbor.

Only DLDP down ports can send and process Recover packets, including RecoverProbe packets and RecoverEcho packets. If related ports are manually shut down with the **shutdown** command, the auto-recovery mechanism will not take effect.

DLDP neighbor state

A DLDP neighbor can be in one of the three states described in Table 17.

Table 17 Description on DLDP neighbor states

DLDP neighbor state	Description
Unknown	A neighbor is in this state when it is just detected and is being probed. A neighbor is in this state only when it is being probed. It transits to Two way state or Unidirectional state after the probe operation finishes.
Two way	A neighbor is in this state after it receives response from its peer. This state indicates the link is a two-way link.
Unidirectional	A neighbor is in this state when the link connecting it is detected to be a unidirectional link. After a device transits to this state, the corresponding neighbor entries maintained on other devices are removed.

DLDP configuration task list

For DLDP to work properly, enable DLDP on both sides and make sure these settings are consistent: the interval to send Advertisement packets, DLDP authentication mode, and password.

DLDP does not process any link aggregation control protocol (LACP) events. The links in an aggregation are treated as individual links in DLDP.

Make sure the DLDP version running on devices on the two ends are the same.

Complete the following tasks to configure DLDP:

Task	Remarks
Configuring the duplex mode and speed of an Ethernet interface	Required
Enabling DLDP	Required
Setting DLDP mode	Optional
Setting the interval to send advertisement packets	Optional
Setting the delaydown timer	Optional
Setting the port shutdown mode	Optional
Configuring DLDP authentication	Optional
Resetting DLDP state	Optional

Configuring the duplex mode and speed of an Ethernet interface

To make sure that DLDP works properly on a link, you must configure the full duplex mode for the ports at two ends of the link, and configure a speed for the two ports, rather than letting them negotiate a speed.

For more information about the **duplex** and **speed** commands, see *Layer 2—LAN Switching Command Reference*.

Enabling DLDP

To properly configure DLDP on the device, first enable DLDP globally, and then enable it on each port.

To enable DLDP:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable DLDP globally.	**dldp enable**	Globally disabled by default.
3.	Enter Layer 2 Ethernet interface view or port group view.	Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* Enter port group view: **port-group manual** *port-group-name*	Use either approach. Configurations made in Layer 2 Ethernet interface view apply to the current port only. Configurations made in port group view apply to all ports in the port group.
4.	Enable DLDP.	**dldp enable**	Disabled on a port by default.

NOTE:

- DLDP takes effect only on Ethernet interfaces (fiber or copper).
- DLDP can detect unidirectional links only after all physical links are connected. Therefore, before enabling DLDP, make sure that optical fibers or copper twisted pairs are connected.

Setting DLDP mode

DLDP operates in normal or enhanced mode.

In normal mode, DLDP does not actively detect neighbors when the corresponding neighbor entries age out.

In enhanced mode, DLDP actively detects neighbors when the corresponding neighbor entries age out.

To set DLDP mode:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Set DLDP mode.	**dldp work-mode** { **enhance** | **normal** }	Optional. Normal by default.

Setting the interval to send advertisement packets

DLDP detects unidirectional links by sending Advertisement packets. To make sure that DLDP can detect unidirectional links promptly without affecting network performance, set the advertisement interval appropriately depending on your network environment. The interval should be set shorter than one third of the STP convergence time. If the interval is too long, STP loops may occur before unidirectional links are detected and shut down. If the interval is too short, the number of advertisement packets will increase. HP recommends that you use the default interval in most cases.

To set the interval to send Advertisement packets:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Set the interval to send Advertisement packets.	**dldp interval** *time*	Optional. 5 seconds by default.

NOTE:

- The interval for sending Advertisement packets applies to all DLDP-enabled ports.
- To enable DLDP to operate properly, make sure the intervals for sending Advertisement packets on both sides of a link are the same.

Setting the delaydown timer

On some ports, when the Tx line fails, the port goes down and then comes up again, causing optical signal jitters on the Rx line. When a port goes down due to a Tx failure, the device transits to the DelayDown state instead of the Inactive state to prevent the corresponding neighbor entries from being removed. At the same time, the device triggers the DelayDown timer. If the port goes up before the timer expires, the device restores the original state; if the port remains down when the timer expires, the device transits to the Inactive state.

To set the DelayDown timer:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Set the DelayDown timer.	**dldp delaydown-timer** *time*	Optional. 1 second by default.

NOTE:

DelayDown timer setting applies to all DLDP-enabled ports.

Setting the port shutdown mode

On detecting a unidirectional link, the ports can be shut down in one of the following two modes:

- **Manual mode**—This mode applies to low performance networks, where normal links may be treated as unidirectional links. It protects data traffic transmission against false unidirectional links. In this mode, DLDP only detects unidirectional links but does not automatically shut down unidirectional link ports. Instead, the DLDP state machine generates log and traps to prompt you to manually shut down unidirectional link ports with the **shutdown** command. HP recommends that you do as prompted. Then the DLDP state machine transits to the Disable state.
- **Auto mode**—In this mode, when a unidirectional link is detected, DLDP transits to Disable state, generates log and traps, and sets the port state to DLDP Down.

On a port with both remote OAM loopback and DLDP enabled, if the port shutdown mode is auto mode, the port will be shut down by DLDP when it receives a packet sent by itself, causing remote OAM loopback to operate improperly. To prevent this, set the port shutdown mode to manual mode.

If the device is busy, or the CPU usage is high, normal links may be treated as unidirectional links. In this case, you can set the port shutdown mode to manual mode to alleviate the impact caused by false unidirectional link report.

To set port shutdown mode:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Set port shutdown mode.	**dldp unidirectional-shutdown** { **auto** | **manual** }	Optional. **auto** by default.

Configuring DLDP authentication

You can guard your network against attacks and malicious probes by configuring an appropriate DLDP authentication mode, which can be simple authentication or MD5 authentication. If your network is safe, you can choose not to authenticate.

To enable DLDP to operate properly, make sure that DLDP authentication modes and passwords on both sides of a link are the same.

To configure DLDP authentication:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Configure DLDP authentication.	**dldp authentication-mode** { **none** | { **md5** | **simple** } *password* }	**none** by default.

Resetting DLDP state

After DLDP detects a unidirectional link on a port, the port enters Disable state. In this case, DLDP prompts you to shut down the port manually or it shuts down the port automatically depending on the user-defined port shutdown mode. To enable the port to perform DLDP detect again, you can reset the DLDP state of the port by using one of the following methods:

- If the port is shut down with the **shutdown** command manually, run the **undo shutdown** command on the port.
- If DLDP automatically shuts down the port, run the **dldp reset** command on the port to enable the port to perform DLDP detection again. Alternatively, you can wait for DLDP to automatically enable the port when it detects that the link has been restored to bidirectional. For how to reset the DLDP state by using the **dldp reset** command, see "Resetting DLDP state in system view" and "Resetting DLDP state in interface view/port group view."

The DLDP state that the port transits to upon the DLDP state reset operation depends on its physical state. If the port is physically down, it transits to Inactive state; if the port is physically up, it transits to Active state.

Resetting DLDP state in system view

Resetting DLDP state in system view applies to all ports of the device.

To reset DLDP in system view:

Step	Command
1. Enter system view.	**system-view**
2. Reset DLDP state.	**dldp reset**

Resetting DLDP state in interface view/port group view

Resetting DLDP state in interface view or port group view applies to the current port or all ports in the port group.

To reset DLDP state in interface view/port group view:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view or port group view.	Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* Enter port group view: **port-group manual** *port-group-name*	Use either approach. Configurations made in Layer 2 Ethernet interface view apply to the current port only. Configurations made in port group view apply to all the ports in the port group.
3. Reset DLDP state.	**dldp reset**	N/A

Displaying and maintaining DLDP

Task	Command	Remarks
Display the DLDP configuration of a port.	**display dldp** [*interface-type interface-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the statistics on DLDP packets passing through a port.	**display dldp statistics** [*interface-type interface-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear the statistics on DLDP packets passing through a port.	**reset dldp statistics** [*interface-type interface-number*]	Available in user view

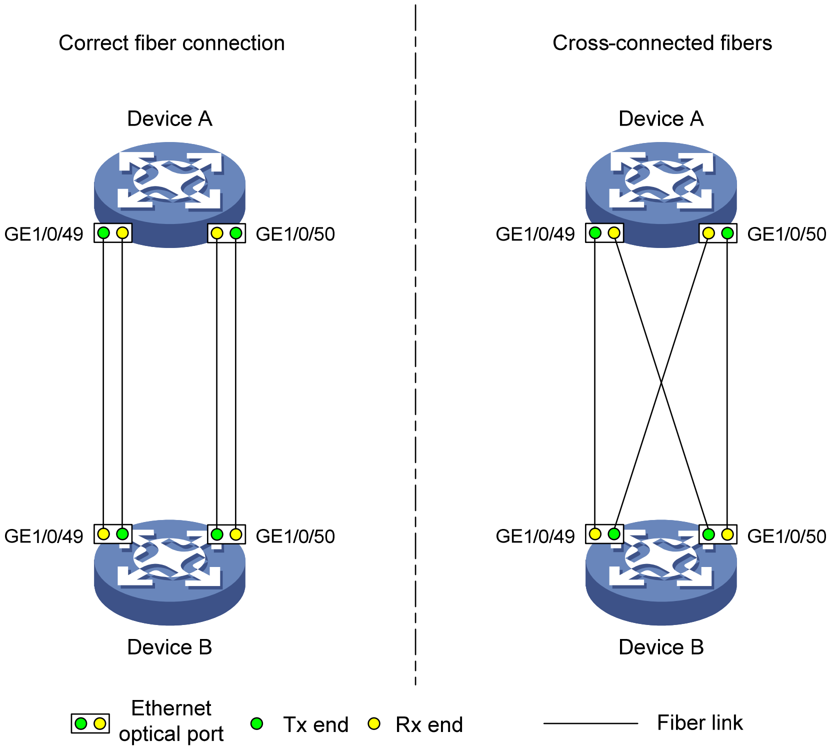
DLDP configuration examples

Automatically shutting down unidirectional links

Network requirements

- As shown in Figure 9, Device A and Device B are connected with two fiber pairs.
- Configure DLDP to automatically shut down the faulty port upon detecting a unidirectional link, and automatically bring up the port after you clear the fault.

Figure 9 Network diagram



Configuration procedure

1. Configure Device A:

   # Enable DLDP globally.

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

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

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

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

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

   # Set the DLDP mode to enhanced.

```
[DeviceA] dldp work-mode enhance
```

   # Set the port shutdown mode to auto.

```
[DeviceA] dldp unidirectional-shutdown auto
```

2. Configure Device B:

# Enable DLDP globally.

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

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

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

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

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

# Set the DLDP mode to enhanced.

```
[DeviceB] dldp work-mode enhance
```

# Set the port shutdown mode to auto.

```
[DeviceB] dldp unidirectional-shutdown auto
```

3. Verify the configuration:

   After the configurations are complete, you can use the **display dldp** command to display the DLDP configuration information on ports.

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

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

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

Interface GigabitEthernet1/0/50
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
```

```
         Neighbor mac address : 0023-8956-3600
         Neighbor port index : 60
         Neighbor state : two way
         Neighbor aged time : 12
```

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

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

```
[DeviceA] quit
<DeviceA> terminal monitor
<DeviceA> terminal logging
<DeviceA> terminal trapping
```

The following log and trap information is displayed on Device A:

```
<DeviceA>
#Jan 18 17:36:18:798 2010 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1<hhpDLDPUnidirectionalPort> : DLDP detects a
unidirectional link in port 17825792.

%Jan 18 17:36:18:799 2010 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link
status is DOWN.
%Jan 18 17:36:18:799 2010 DeviceA DLDP/3/DLDP_UNIDIRECTION_AUTO: -Slot=1; DLDP
detects a unidirectional link on port GigabitEthernet1/0/49. The transceiver has
malfunction in the Tx direction or cross-connected links exist between the local device
and its neighbor. The shutdown mode is AUTO. DLDP shuts down the port.
#Jan 18 17:36:20:189 2010 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1<hhpDLDPUnidirectionalPort> : DLDP detects a
unidirectional link in port 17825793.

%Jan 18 17:36:20:189 2010 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link
status is DOWN.
%Jan 18 17:36:20:190 2010 DeviceA DLDP/3/DLDP_UNIDIRECTION_AUTO: -Slot=1; DLDP
detects a unidirectional link on port GigabitEthernet1/0/50. The transceiver has
malfunction in the Tx direction or cross-connected links exist between the local device
and its neighbor. The shutdown mode is AUTO. DLDP shuts down the port.

%Jan 15 16:54:56:040 2010 DeviceA DLDP/3/DLDP_UNIDIRECTION_AUTO_ENHANCE: -Slot=1; In
enhanced DLDP mode, port GigabitEthernet1/0/49 cannot detect its aged-out neighbor.
The transceiver has malfunction in the Tx direction or cross-connected links exist
between the local device and its neighbor. The shutdown mode is AUTO. DLDP shuts down
the port.
```

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

Assume that in this example, the unidirectional links are caused by cross-connected fibers. Correct the fiber connections on detecting the unidirectional link problem. As a result, the ports shut down by DLDP automatically recover, and Device A displays the following log information:

```
<DeviceA>
%Jan 18 17:47:33:869 2010 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link
status is UP.
```

```
%Jan 18 17:47:35:894 2010 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link
status is UP.
```

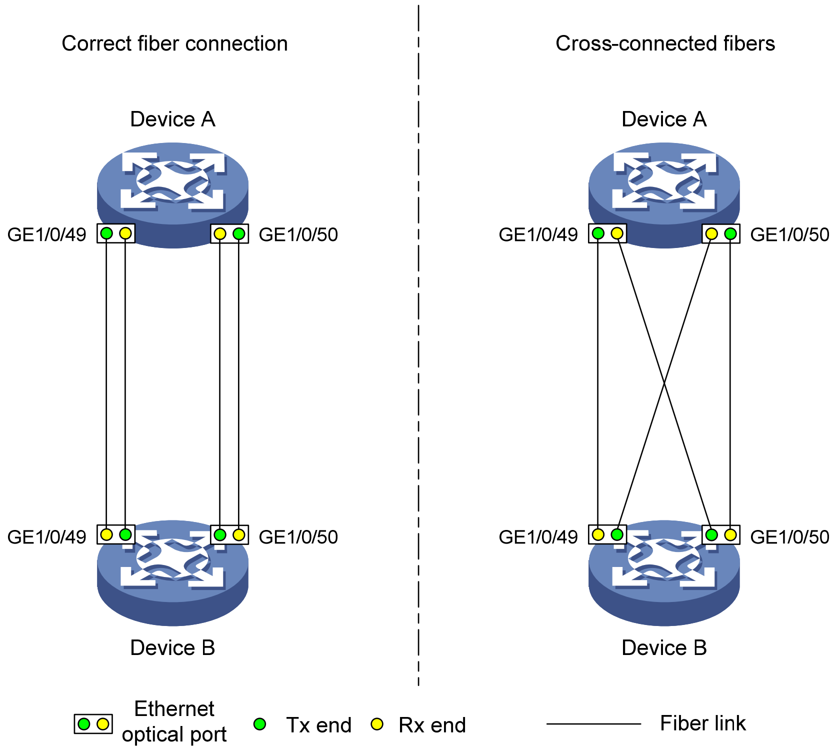
The output shows that the link status of both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 is now up.

Manually shutting down unidirectional links

Network requirements

- As shown in Figure 10, Device A and Device B are connected with two fiber pairs.
- Configure DLDP to send information when a unidirectional link is detected, to remind the network administrator to manually shut down the faulty port.

Figure 10 Network diagram



Configuration procedure

1. Configure Device A:

# Enable DLDP globally.

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

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

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

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

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

# Set the DLDP mode to enhanced.

```
[DeviceA] dldp work-mode enhance
```

# Set the port shutdown mode to manual.

```
[DeviceA] dldp unidirectional-shutdown manual
```

2. Configure Device B:

# Enable DLDP globally.

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

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

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

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

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

# Set the DLDP mode to enhanced.

```
[DeviceB] dldp work-mode enhance
```

# Set the port shutdown mode to manual.

```
[DeviceB] dldp unidirectional-shutdown manual
```

3. Verify the configuration:

After the configurations are complete, you can use the **display dldp** command to display the DLDP configuration information on ports.

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

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

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

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

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

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

```
[DeviceA] quit
<DeviceA> terminal monitor
<DeviceA> terminal logging
<DeviceA> terminal trapping
```

The following log and trap information is displayed on Device A:

```
<DeviceA>
#Jan 18 18:10:38:481 2010 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1<hhpDLDPUnidirectionalPort> : DLDP detects a
unidirectional link in port 17825792.

%Jan 18 18:10:38:481 2010 DeviceA DLDP/3/DLDP_UNIDIRECTION_MANUAL: -Slot=1; DLDP
detects a unidirectional link on port GigabitEthernet1/0/49. The transceiver has
malfunction in the Tx direction or cross-connected links exist between the local device
and its neighbor. The shutdown mode is MANUAL. The port needs to be shut down by the
user.
#Jan 18 18:10:38:618 2010 DeviceA DLDP/1/TrapOfUnidirectional: -Slot=1; Trap
1.3.6.1.4.1.25506.2.43.2.1.1<hhpDLDPUnidirectionalPort> : DLDP detects a
unidirectional link in port 17825793.

%Jan 18 18:10:38:618 2010 DeviceA DLDP/3/DLDP_UNIDIRECTION_MANUAL: -Slot=1; DLDP
detects a unidirectional link on port GigabitEthernet1/0/50. The transceiver has
malfunction in the Tx direction or cross-connected links exist between the local device
and its neighbor. The shutdown mode is MANUAL. The port needs to be shut down by the
user.
```

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

After you shut down GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50, the following log information is displayed:

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

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

Assume that in this example, the unidirectional links are caused by cross-connected fibers. Correct the fiber connections, and then bring up the ports shut down earlier.

# On Device A, bring up GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50:

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

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

Troubleshooting DLDP

Symptom

Two DLDP-enabled devices, Device A and Device B, are connected through two fiber pairs, in which two fibers are cross-connected. The unidirectional links cannot be detected; all the four ports involved are in Advertisement state.

Analysis

The problem can be caused by the following.

- The intervals to send Advertisement packets on Device A and Device B are not the same.
- DLDP authentication modes/passwords on Device A and Device B are not the same.

Solution

Make sure the interval to send Advertisement packets, the authentication mode, and the password configured on Device A and Device B are the same.

Configuring RRPP

RRPP overview

The Rapid Ring Protection Protocol (RRPP) is a link layer protocol designed for Ethernet rings. RRPP can prevent broadcast storms caused by data loops when an Ethernet ring is healthy, and rapidly restore the communication paths between the nodes in the event that a link is disconnected on the ring.

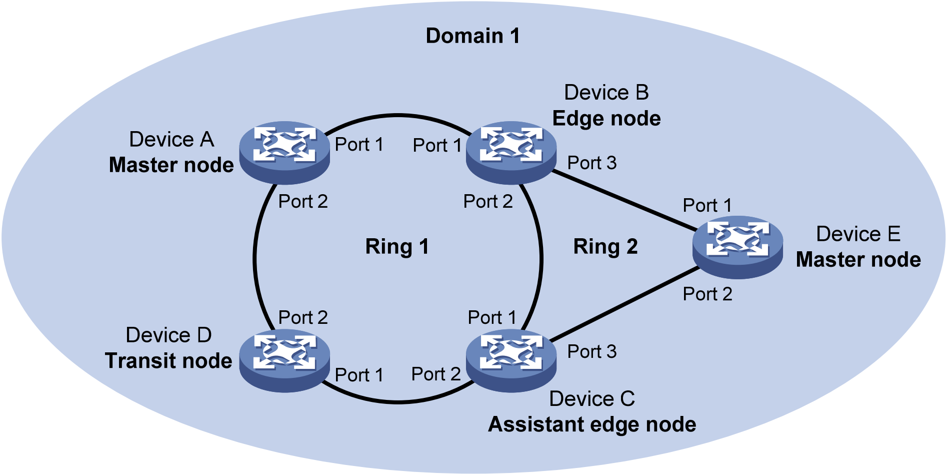
Background

Metropolitan area networks (MANs) and enterprise networks usually use the ring structure to improve reliability. However, services will be interrupted if any node in the ring network fails. A ring network usually uses Resilient Packet Ring (RPR) or Ethernet rings. RPR is high in cost because it needs dedicated hardware. Contrarily, the Ethernet ring technology is more mature and economical, so it is increasingly widely used in MANs and enterprise networks.

Rapid Spanning Tree Protocol (RSTP), Per VLAN Spanning Tree (PVST), Multiple Spanning Tree Protocol (MSTP), and RRPP can eliminate Layer-2 loops. RSTP, PVST, and MSTP are mature. However, they take several seconds to converge. RRPP is an Ethernet ring-specific data link layer protocol, and it converges faster than RSTP, PVST, and MSTP. Additionally, the convergence time of RRPP is independent of the number of nodes in the Ethernet ring. RRPP can be applied to large-diameter networks.

Basic concepts in RRPP

Figure 11 RRPP networking diagram



RRPP domain

The interconnected devices with the same domain ID and control VLANs constitute an RRPP domain. An RRPP domain contains the following elements—primary ring, subring, control VLAN, master node, transit node, primary port, secondary port, common port, edge port, and so on.

As shown in Figure 11, Domain 1 is an RRPP domain, including two RRPP rings: Ring 1 and Ring 2. All the nodes on the two RRPP rings belong to the RRPP domain.

RRPP ring

A ring-shaped Ethernet topology is called an "RRPP ring". RRPP rings fall into two types: primary ring and subring. You can configure a ring as either the primary ring or a subring by specifying its ring level. The primary ring is of level 0, and a subring is of level 1. An RRPP domain contains one or multiple RRPP rings, one serving as the primary ring and the others serving as subrings. A ring can be in one of the following states:

- **Health state**—All the physical links on the Ethernet ring are connected
- **Disconnect state**—Some physical links on the Ethernet ring are broken

As shown in Figure 11, Domain 1 contains two RRPP rings: Ring 1 and Ring 2. The level of Ring 1 is set to 0, and that of Ring 2 is set to 1. Ring 1 is configured as the primary ring, and Ring 2 is configured as a subring.

Control VLAN and data VLAN

1. Control VLAN

   In an RRPP domain, a control VLAN is a VLAN dedicated to transferring Rapid Ring Protection Protocol Data Units (RRPPDUs). On a device, the ports accessing an RRPP ring belong to the control VLANs of the ring, and only such ports can join the control VLANs.

   An RRPP domain is configured with two control VLANs: one primary control VLAN, which is the control VLAN for the primary ring, and one secondary control VLAN, which is the control VLAN for subrings. All subrings in the same RRPP domain share the same secondary control VLAN. After you specify a VLAN as the primary control VLAN, the system automatically configures the VLAN whose ID is the primary control VLAN ID plus one as the secondary control VLAN.

   IP address configuration is prohibited on the control VLAN interfaces.

2. Data VLAN

   A data VLAN is a VLAN dedicated to transferring data packets. Both RRPP ports and non-RRPP ports can be assigned to a data VLAN.

Node

Each device on an RRPP ring is a node. The role of a node is configurable. RRPP has the following node roles:

- **Master node**—Each ring has one and only one master node. The master node initiates the polling mechanism and determines the operations to be performed after a change in topology.
- **Transit node**—Transit nodes include all the nodes except the master node on the primary ring and all the nodes on subrings except the master nodes and the nodes where the primary ring intersects with the subrings. A transit node monitors the state of its directly-connected RRPP links and notifies the master node of the link state changes, if any. Based on the link state changes, the master node decides the operations to be performed.
- **Edge node**—A special node residing on both the primary ring and a subring at the same time. An edge node serves as a master node or a transit node on the primary ring and an edge node on the subring.
- **Assistant-edge node**—A special node residing on both the primary ring and a subring at the same time. An assistant-edge node serves as a master node or a transit node on the primary ring and an assistant-edge node on the subring. This node works in conjunction with the edge node to detect the integrity of the primary ring and to perform loop guard.

As shown in Figure 11, Ring 1 is the primary ring and Ring 2 is a subring. Device A is the master node of Ring 1, and Device B, Device C, and Device D are the transit nodes of Ring 1. Device E is the master node of Ring 2, Device B is the edge node of Ring 2, and Device C is the assistant-edge node of Ring 2.

Primary port and secondary port

Each master node or transit node has two ports connected to an RRPP ring, one serving as the primary port and the other serving as the secondary port. You can determine the port's role.

1. In terms of functionality, the primary port and the secondary port of a master node have the following differences:
    - The primary port and the secondary port are designed to play the role of sending and receiving loop-detect packets respectively.
    - When an RRPP ring is in Health state, the secondary port of the master node will logically deny data VLANs and permit only the packets of the control VLANs.
    - When an RRPP ring is in Disconnect state, the secondary port of the master node will permit data VLANs (forward packets of data VLANs).
2. In terms of functionality, the primary port and the secondary port of a transit node have no difference. Both are designed for transferring protocol packets and data packets over an RRPP ring.

As shown in Figure 11, Device A is the master node of Ring 1. Port 1 and Port 2 are the primary port and the secondary port of the master node on Ring 1 respectively. Device B, Device C, and Device D are the transit nodes of Ring 1. Their Port 1 and Port 2 are the primary port and the secondary port on Ring 1 respectively.

Common port and edge port

The ports connecting the edge node and assistant-edge node to the primary ring are common ports. The ports connecting the edge node and assistant-edge node only to the subrings are edge ports.

As shown in Figure 11, Device B and Device C lie on Ring 1 and Ring 2. Device B's Port 1 and Port 2 and Device C's Port 1 and Port 2 access the primary ring, so they are common ports. Device B's Port 3 and Device C's Port 3 access only the subring, so they are edge ports.

RRPP ring group

To reduce Edge-Hello traffic, you can configure a group of subrings on the edge node or assistant-edge node. For more information about Edge-Hello packets, see "RRPPDUS." You must configure a device as the edge node of these subrings, and another device as the assistant-edge node of these subrings. Additionally, the subrings of the edge node and assistant-edge node must connect to the same subring packet tunnels in major ring (SRPTs) so that Edge-Hello packets of the edge node of these subrings travel to the assistant-edge node of these subrings over the same link.

An RRPP ring group configured on the edge node is an edge node RRPP ring group, and an RRPP ring group configured on an assistant-edge node is an assistant-edge node RRPP ring group. Up to one subring in an edge node RRPP ring group is allowed to send Edge-Hello packets.

RRPPDUS

Table 18 RRPPDU types and their functions

Type	Description
Hello	The master node initiates Hello packets to detect the integrity of a ring in a network.
Link-Down	The transit node, the edge node, or the assistant-edge node initiates Link-Down packets to notify the master node of the disappearance of a ring in case of a link failure.

Type	Description
Common-Flush-FDB	The master node initiates Common-Flush-FDB packets to instruct the transit nodes to update their own MAC entries and ARP/ND entries when an RRPP ring transits to Disconnect state. FDB stands for Forwarding Database.
Complete-Flush-FDB	The master node initiates Complete-Flush-FDB packets to instruct the transit nodes to update their own MAC entries and ARP/ND entries and release blocked ports from being blocked temporarily when an RRPP ring transits to Health state.
Edge-Hello	The edge node initiates Edge-Hello packets to examine the SRPTs between the edge node and the assistant-edge node.
Major-Fault	The assistant-edge node initiates Major-Fault packets to notify the edge node of SRPT failure when an SRPT between edge node and assistant-edge node is torn down.

NOTE:

RRPPDUs of subrings are transmitted as data packets in the primary ring, and RRPPDUs of the primary ring can only be transmitted within the primary ring.

RRPP timers

When RRPP checks the link state of an Ethernet ring, the master node sends Hello packets out of the primary port according to the Hello timer and determines whether its secondary port receives the Hello packets based on the Fail timer.

- The Hello timer specifies the interval at which the master node sends Hello packets out of the primary port.
- The Fail timer specifies the maximum delay between the master node sending Hello packets out of the primary port and the secondary port receiving the Hello packets from the primary port. If the secondary port receives the Hello packets sent by the local master node before the Fail timer expires, the overall ring is in Health state. Otherwise, the ring transits into the Disconnect state.

NOTE:

In an RRPP domain, a transit node learns the Hello timer value and the Fail timer value on the master node through the received Hello packets, ensuring that all nodes in the ring network are consistent in the two timer settings.

How RRPP works

Polling mechanism

The polling mechanism is used by the master node of an RRPP ring to check the Health state of the ring network.

The master node periodically sends Hello packets out of its primary port, and these Hello packets travel through each transit node on the ring in turn:

- If the ring is complete, the secondary port of the master node will receive Hello packets before the Fail timer expires and the master node will keep the secondary port blocked.
- If the ring is torn down, the secondary port of the master node will fail to receive Hello packets before the Fail timer expires. The master node will release the secondary port from blocking data

VLANs and sending Common-Flush-FDB packets to instruct all transit nodes to update their own MAC entries and ARP/ND entries.

Link down alarm mechanism

The transit node, the edge node or the assistant-edge node sends Link-Down packets to the master node immediately when they find any of its own ports belonging to an RRPP domain are down. Upon the receipt of a Link-Down packet, the master node releases the secondary port from blocking data VLANs and sending Common-Flush-FDB packet to instruct all the transit nodes, the edge nodes, and the assistant-edge nodes to update their own MAC entries and ARP/ND entries. After each node updates its own entries, traffic is switched to the normal link.

Ring recovery

The master node may find that the ring is restored after a period of time after the ports belonging to the RRPP domain on the transit nodes, the edge nodes, or the assistant-edge nodes are brought up again. A temporary loop may arise in the data VLAN during this period. As a result, broadcast storm occurs.

To prevent temporary loops, non-master nodes block them immediately (and permit only the packets of the control VLAN to pass through) when they find their ports accessing the ring are brought up again. The blocked ports are activated only when the nodes are sure that no loop will be brought forth by these ports.

Broadcast storm suppression mechanism in a multi-homed subring in case of SRPT failure

As shown in Figure 15, Ring 1 is the primary ring, and Ring 2 and Ring 3 are subrings. When the two SRPTs between the edge node and the assistant-edge node are down, the master nodes of Ring 2 and Ring 3 will open their respective secondary ports, generating a loop among Device B, Device C, Device E, and Device F. As a result, a broadcast storm occurs.

To prevent generating this loop, the edge node will block the edge port temporarily. The blocked edge port is activated only when the edge node is sure that no loop will be brought forth when the edge port is activated.

Load balancing

In a ring network, maybe traffic of multiple VLANs is transmitted at the same time. RRPP can implement load balancing for the traffic by transmitting traffic of different VLANs along different paths.

By configuring an individual RRPP domain for transmitting the traffic of the specified VLANs (protected VLANs) in a ring network, traffic of different VLANs can be transmitted according to different topologies in the ring network. In this way, load balancing is achieved.

As shown in Figure 16, Ring 1 is configured as the primary ring of Domain 1 and Domain 2, which are configured with different protected VLANs. Device A is the master node of Ring 1 in Domain 1, and Device B is the master node of Ring 1 in Domain 2. With such configurations, traffic of different VLANs can be transmitted on different links to achieve load balancing in the single-ring network.

RRPP ring group

In an edge node RRPP ring group, only an activated subring with the lowest domain ID and ring ID can send Edge-Hello packets. In an assistant-edge node RRPP ring group, any activated subring that has received Edge-Hello packets will forward these packets to the other activated subrings. With an edge node RRPP ring group and an assistant-edge node RRPP ring group configured, only one subring sends Edge-Hello packets on the edge node, and only one subring receives Edge-Hello packets on the assistant-edge node, reducing CPU workload.

As shown in Figure 15, Device B is the edge node of Ring 2 and Ring 3, and Device C is the assistant-edge node of Ring 2 and Ring 3. Device B and Device C must send or receive Edge-Hello packets frequently. If more subrings are configured or if load balancing is configured for multiple domains, Device B and Device C will send or receive a mass of Edge-Hello packets.

To reduce Edge-Hello traffic, you can assign Ring 2 and Ring 3 to an RRPP ring group configured on the edge node Device B and assign Ring 2 and Ring 3 to an RRPP ring group configured on Device C. After such configurations, if all rings are activated, only Ring 2 on Device B sends Edge-Hello packets.

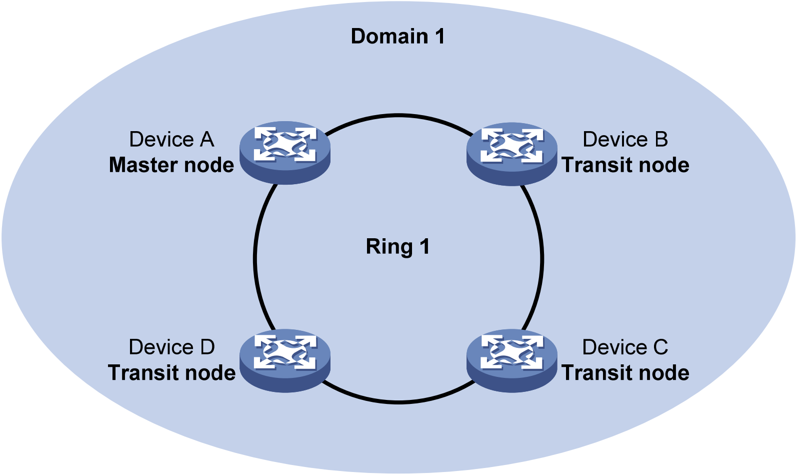
Typical RRPP networking

Here are several typical networking applications.

Single ring

As shown in Figure 12, only a single ring exists in the network topology. You only need to define an RRPP domain.

Figure 12 Schematic diagram for a single-ring network



Tangent rings

As shown in Figure 13, two or more rings are in the network topology and only one common node exists between rings. You must define an RRPP domain for each ring.

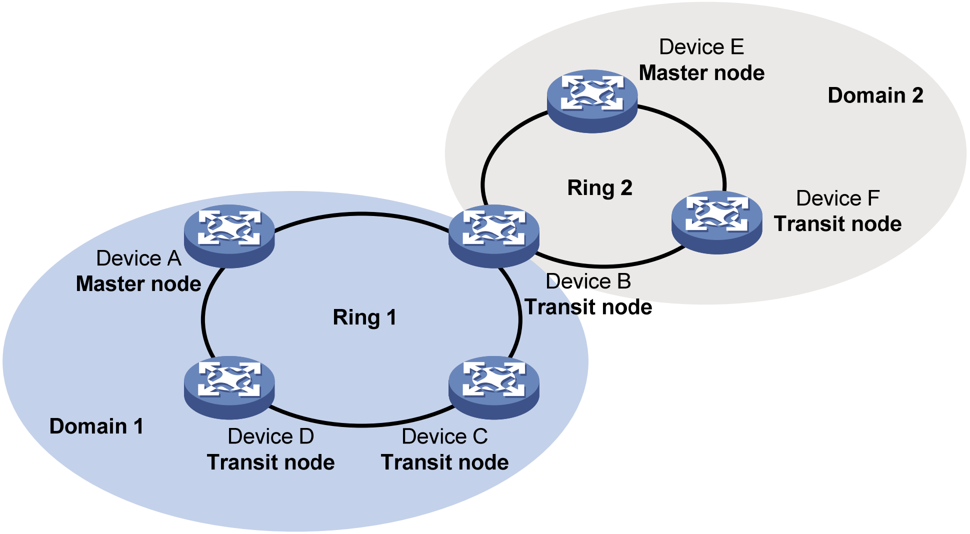
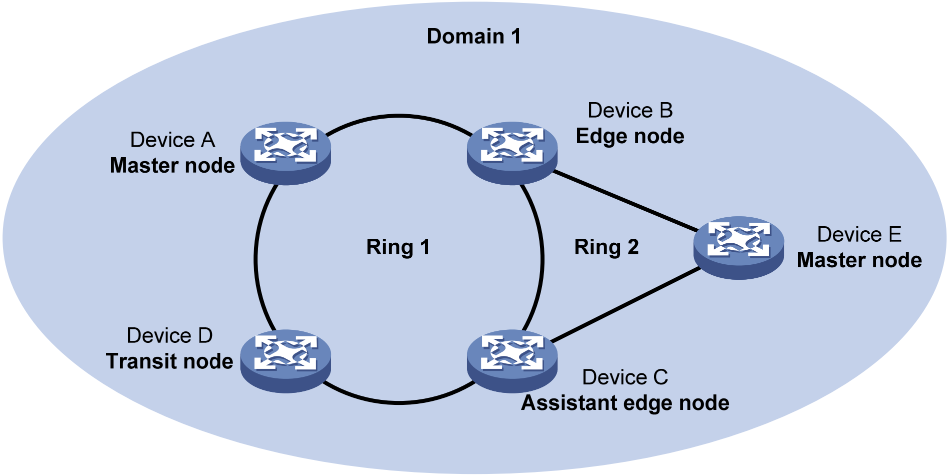


Figure 13 Schematic diagram for a tangent-ring network

Intersecting rings

As shown in Figure 14, two or more rings are in the network topology and two common nodes exist between rings. You only need to define an RRPP domain and configure one ring as the primary ring and the other rings as subrings.

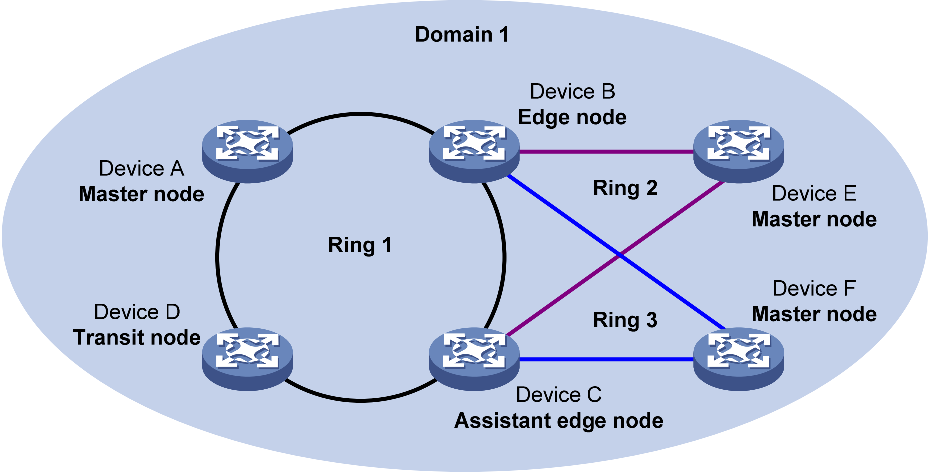
Figure 14 Schematic diagram for an intersecting-ring network



Dual homed rings

As shown in Figure 15, two or more rings are in the network topology and two similar common nodes exist between rings. You only need to define an RRPP domain and configure one ring as the primary ring and the other rings as subrings.

Figure 15 Schematic diagram for a dual-homed-ring network

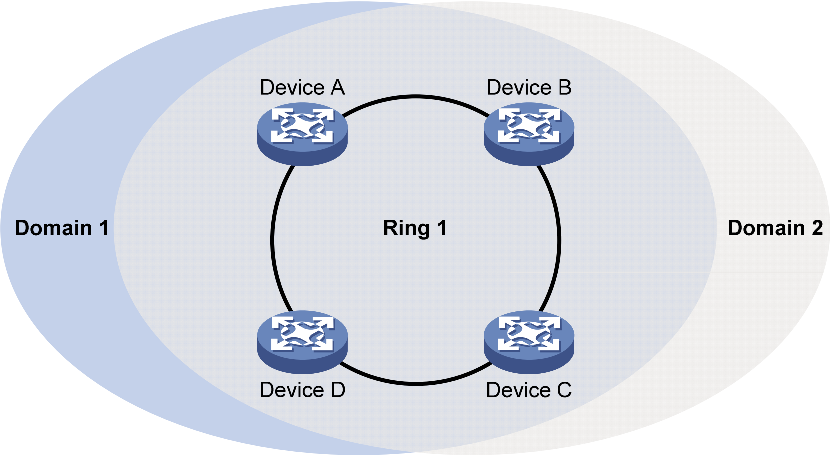


Single-ring load balancing

In a single-ring network, you can achieve load balancing by configuring multiple domains.

As shown in Figure 16, Ring 1 is configured as the primary ring of both Domain 1 and Domain 2. Domain 1 and Domain 2 are configured with different protected VLANs. In Domain 1, Device A is configured as the master node of Ring 1. In Domain 2, Device B is configured as the master node of Ring 1. Such configurations enable the ring to block different links based on VLANs, and single-ring load balancing is achieved.

Figure 16 Schematic diagram for a single-ring load balancing network

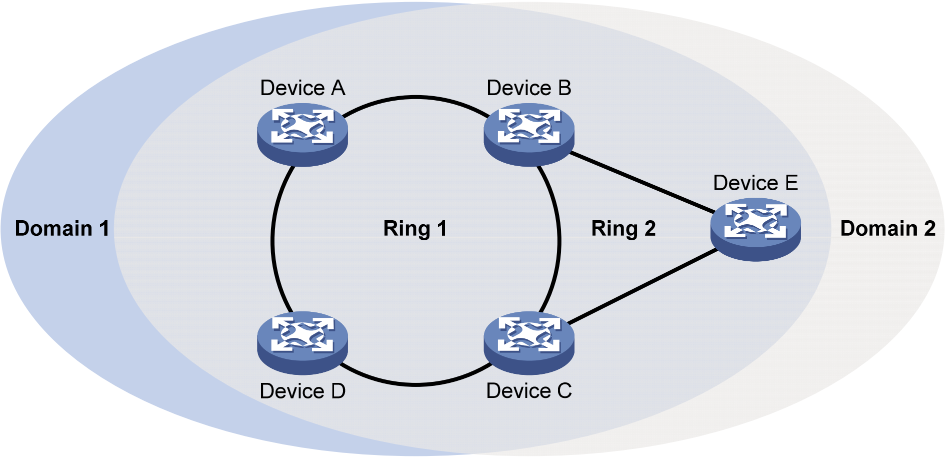


Intersecting-ring load balancing

In an intersecting-ring network, you can also achieve load balancing by configuring multiple domains.

As shown in Figure 17, Ring 1 is the primary ring, and Ring 2 is the subring in both Domain 1 and Domain 2. Domain 1 and Domain 2 are configured with different protected VLANs. Device A is configured as the master node of Ring 1 in Domain 1. Device D is configured as the master node of Ring 1 in Domain 2. Device E is configured as the master node of Ring 2 in both Domain 1 and Domain 2. However, different ports on Device E are blocked in Domain 1 and Domain 2. With the configurations, you can enable traffic of different VLANs to travel over different paths in the subring and primary ring to achieve intersecting-ring load balancing.

Figure 17 Schematic diagram for an intersecting-ring load balancing network



Protocols and standards

RFC 3619 *Extreme Networks' Ethernet Automatic Protection Switching (EAPS) Version 1* is related to RRPP.

RRPP configuration task list

You can create RRPP domains based on service planning, specify control VLANs and data VLANs for each RRPP domain, and then determine the ring roles and node roles based on the traffic paths in each RRPP domain.

Complete the following tasks to configure RRPP:

Task		Remarks
Creating an RRPP domain		Required. Perform this task on all nodes in the RRPP domain.
Configuring control VLANs		Required. Perform this task on all nodes in the RRPP domain.
Configuring protected VLANs		Required. Perform this task on all nodes in the RRPP domain.
Configuring RRPP rings	Configuring RRPP ports	Required. Perform this task on all nodes in the RRPP domain.
	Configuring RRPP nodes	Required. Perform this task on all nodes in the RRPP domain
Activating an RRPP domain		Required. Perform this task on all nodes in the RRPP domain.
Configuring RRPP timers		Optional. Perform this task on the master node in the RRPP domain.

Task	Remarks
Configuring an RRPP ring group	Optional. Perform this task on the edge node and assistant-edge node in the RRPP domain.

NOTE:

- RRPP does not have an auto election mechanism, so you must configure each node in the ring network properly for RRPP to monitor and protect the ring network.
- Before configuring RRPP, you must construct a ring-shaped Ethernet topology physically.

Creating an RRPP domain

When creating an RRPP domain, specify a domain ID, which uniquely identifies an RRPP domain. All devices in the same RRPP domain must be configured with the same domain ID.

Perform this configuration on devices you want to configure as nodes in the RRPP domain.

To create an RRPP domain:

Step		Command
1.	Enter system view.	**system-view**
2.	Create an RRPP domain, and enter RRPP domain view.	**rrpp domain** *domain-id*

Configuring control VLANs

Before configuring RRPP rings in an RRPP domain, configure the same control VLANs for all nodes in the RRPP domain first. When configuring control VLANs for an RRPP domain, you only need to configure the primary control VLAN. The system automatically configures the secondary control VLAN, and it uses the primary control VLAN ID plus 1 as the secondary control VLAN ID. For the control VLAN configuration to succeed, make sure the IDs of the two control VLANs are consecutive and have not been assigned yet.

Perform this configuration on all nodes in the RRPP domain to be configured.

Configuration guidelines

- To ensure proper forwarding of RRPPDUs, do not configure the default VLAN of a port accessing an RRPP ring as the control VLAN, or enable 802.1Q in 802.1Q (QinQ) or VLAN mapping on the control VLANs.
- Before configuring RRPP rings for an RRPP domain, you can delete or modify the control VLANs configured for the RRPP domain. However, after configuring RRPP rings for an RRPP domain, you cannot delete or modify the control VLANs of the domain. You can only use the **undo control-vlan** command to delete a control VLAN.
- To transparently transmit RRPPDUs on a device not configured with RRPP, you must ensure only the two ports connecting the device to the RRPP ring permit the packets of the control VLANs. Otherwise, the packets from other VLANs may go into the control VLANs in transparent transmission mode and strike the RRPP ring.

Configuration procedure

To configure control VLANs:

Step	Command
1. Enter system view.	**system-view**
2. Enter RRPP domain view.	**rrpp domain** *domain-id*
3. Configure the primary control VLAN for the RRPP domain.	**control-vlan** *vlan-id*

Configuring protected VLANs

Before configuring RRPP rings in an RRPP domain, configure the same protected VLANs for all nodes in the RRPP domain first. All VLANs that the RRPP ports are assigned to should be protected by the RRPP domains.

You can configure protected VLANs through referencing Multiple Spanning Tree Instances (MSTIs). Before configuring protected VLANs, configure the mappings between MSTIs and the VLANs to be protected. (A device working in PVST mode automatically maps VLANs to MSTIs.) For more information about MSTIs and PVST, see *Layer 2—LAN Switching Configuration Guide*.

Perform this configuration on all nodes in the RRPP domain to be configured.

To configure protected VLANs:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter MST region view.	**stp region-configuration**	Not required if the device is operating in PVST mode. For more information about the command, see *Layer 2—LAN Switching Command Reference*.
3. Configure the VLAN-to-instance mapping table.	Approach 1: **instance** *instance-id* **vlan** *vlan-list* Approach 2: **vlan-mapping modulo** *modulo*	Optional. Use either approach. All VLANs in an MST region are mapped to MSTI 0 (the CIST) by default. Not required if the device is operating in PVST mode. For more information about the commands, see *Layer 2—LAN Switching Command Reference*.
4. Activate MST region configuration manually.	**active region-configuration**	Not required if the device is operating in PVST mode. For more information about the command, see *Layer 2—LAN Switching Command Reference*.

Step		Command	Remarks
5.	Display the currently activated configuration information of the MST region.	**display stp region-configuration** [| { **begin** | **exclude** | **include** } *regular-expression*]	Optional. Available in any view. The command output includes VLAN-to-instance mappings. For more information about the command, see *Layer 2—LAN Switching Command Reference*.
6.	Return to system view.	**quit**	Not required if the device is operating in PVST mode.
7.	Enter RRPP domain view.	**rrpp domain** *domain-id*	N/A
8.	Configure protected VLANs for the RRPP domain.	**protected-vlan reference-instance** *instance-id-list*	By default, no protected VLAN is configured for an RRPP domain.

NOTE:

When configuring load balancing, you must configure different protected VLANs for different RRPP domains.

Configuring RRPP rings

When configuring an RRPP ring, you must make some configurations on the ports connecting each node to the RRPP ring before configuring the nodes.

RRPP ports (connecting devices to an RRPP ring) must be Layer-2 Ethernet ports or Layer-2 aggregate interfaces and cannot be member ports of any aggregation group, service loopback group, or smart link group.

After configuring a Layer-2 aggregate interface as an RRPP port, you can still assign ports to or remove ports from the aggregation group corresponding to the interface.

Configuring RRPP ports

Perform this configuration on each node's ports intended for accessing RRPP rings.

Configuration guidelines

- RRPP ports always allow packets of the control VLANs to pass through.
- For more information about the **port link-type trunk**, **port trunk permit vlan**, and **undo stp enable** commands, see *Layer 2—LAN Switching Command Reference*.
- Do not configure a port accessing an RRPP ring as the destination port of a mirroring group.
- Do not configure physical-link-state change suppression time on a port accessing an RRPP ring to accelerate topology convergence. For more information, see the **undo link-delay** command (*Layer 2—LAN Switching Command Reference*).

Configuration procedure

To configure RRPP ports:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter Layer 2 Ethernet interface view or Layer 2 aggregation interface view.	**interface** *interface-type interface-number*	N/A
3.	Configure the link type of the interface as trunk.	**port link-type trunk**	By default, the link type of an interface is access.
4.	Assign the trunk port to the protected VLANs of the RRPP domain.	**port trunk permit vlan** { *vlan-id-list* | **all** }	By default, a trunk port allows only packets of VLAN 1 to pass through.
5.	Disable the spanning tree feature.	**undo stp enable**	Enabled by default.
6.	Configure the port to trust the 802.1p precedence of the received packets.	**qos trust dot1p**	By default, the port priority is trusted.

Configuring RRPP nodes

If a device carries multiple RRPP rings in an RRPP domain, only one ring can be configured as the primary ring on the device, and the role of the device on a subring can only be an edge node or an assistant-edge node.

Specifying a master node

Perform this configuration on a device to be configured as a master node.

To specify a master node:

Step		Command
1.	Enter system view.	**system-view**
2.	Enter RRPP domain view.	**rrpp domain** *domain-id*
3.	Specify the current device as the master node of the ring, and specify the primary port and the secondary port.	**ring** *ring-id* **node-mode master** [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value*

Specifying a transit node

Perform this configuration on a device to be configured as a transit node.

To specify a transit node:

Step		Command
1.	Enter system view.	**system-view**
2.	Enter RRPP domain view.	**rrpp domain** *domain-id*
3.	Specify the current device as a transit node of the ring, and specify the primary port and the secondary port.	**ring** *ring-id* **node-mode transit** [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value*

Specifying an edge node

When configuring an edge node, you must first configure the primary ring before configuring the subrings.

Perform this configuration on a device to be configured as an edge node.

To specify an edge node:

Step		Command
1.	Enter system view.	**system-view**
2.	Enter RRPP domain view.	**rrpp domain** *domain-id*
3.	Specify the current device as a master node or transit node of the primary ring, and specify the primary port and the secondary port.	**ring** *ring-id* **node-mode** { **master** | **transit** } [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value*
4.	Specify the current device as the edge node of a subring, and specify the edge port.	**ring** *ring-id* **node-mode edge** [**edge-port** *interface-type interface-number*]

Specifying an assistant-edge node

When configuring an assistant-edge node, you must first configure the primary ring before configuring the subrings.

Perform this configuration on a device to be configured as an assistant-edge node.

To specify an assistant-edge node:

Step		Command
1.	Enter system view.	**system-view**
2.	Enter RRPP domain view.	**rrpp domain** *domain-id*
3.	Specify the current device as a master node or transit node of the primary ring, and specify the primary port and the secondary port.	**ring** *ring-id* **node-mode** { **master** | **transit** } [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value*
4.	Specify the current device as the assistant-edge node of the subring, and specify an edge port.	**ring** *ring-id* **node-mode assistant-edge** [**edge-port** *interface-type interface-number*]

Activating an RRPP domain

To activate an RRPP domain on the current device, enable the RRPP protocol and RRPP rings for the RRPP domain on the current device.

To prevent Hello packets of subrings from being looped on the primary ring, enable the primary ring on its master node before enabling the subrings on their separate master nodes. On an edge node or assistant-edge node, enable/disable the primary ring and subrings separately:

- Enable the primary ring of an RRPP domain before enabling the subrings of the RRPP domain.
- Disable the primary ring of an RRPP domain after disabling all subrings of the RRPP domain.

Perform this operation on all nodes in the RRPP domain.

To activate an RRPP domain:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable RRPP.	**rrpp enable**	Disabled by default.
3.	Enter RRPP domain view.	**rrpp domain** *domain-id*	N/A
4.	Enable the specified RRPP ring.	**ring** *ring-id* **enable**	Disabled by default.

Configuring RRPP timers

Perform this configuration on the master node of an RRPP domain.

To configure RRPP timers:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter RRPP domain view.	**rrpp domain** *domain-id*	N/A
3.	Configure the Hello timer and Fail timer for the RRPP domain.	**timer hello-timer** *hello-value* **fail-timer** *fail-value*	By default, the Hello timer value is 1 second, and the Fail timer value is 3 seconds.

NOTE:

- The Fail timer value must be equal to or greater than three times the Hello timer value.
- To avoid temporary loops when the primary ring fails in a dual-homed-ring network, make sure that the difference between the Fail timer value on the master node of the subring and that on the master node of the primary ring is greater than twice the Hello timer value of the master node of the subring.

Configuring an RRPP ring group

To reduce Edge-Hello traffic, adopt the RRPP ring group mechanism by assigning subrings with the same edge node/assistant-edge node to an RRPP ring group. An RRPP ring group must be configured on both the edge node and the assistant-edge node and can only be configured on these two types of nodes.

Perform this configuration on both the edge node and the assistant-edge node in an RRPP domain.

Configuration restrictions and guidelines

- You can assign a subring to only one RRPP ring group. Make sure the RRPP ring group configured on the edge node and the RRPP ring group configured on the assistant-edge node contain the same subrings. Otherwise, the RRPP ring group cannot operate properly.
- Make sure the subrings in an RRPP ring group share the same edge node and assistant-edge node and that the edge node and the assistant edge node have the same SRPTs.
- Make sure a device plays the same role on the subrings in an RRPP ring group. The role can be the edge node or the assistant-edge node.
- Make sure the RRPP ring group on the edge node and the RRPP ring group on the assistant-edge node have the same configurations and activation status.

- Make sure that all subrings in an RRPP ring group have the same SRPTs. If the SRPTs of these subrings are configured or modified differently, the RRPP ring group cannot operate properly.

Configuration procedure

To configure an RRPP ring group:

Step	Command
1. Enter system view.	**system-view**
2. Create an RRPP ring group and enter RRPP ring group view.	**rrpp ring-group** *ring-group-id*
3. Assign the specified subrings to the RRPP ring group.	**domain** *domain-id* **ring** *ring-id-list*

Displaying and maintaining RRPP

Task	Command	Remarks
Display brief RRPP information.	**display rrpp brief** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display RRPP group configuration information.	**display rrpp ring-group** [*ring-group-id*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display detailed RRPP information.	**display rrpp verbose domain** *domain-id* [**ring** *ring-id*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display RRPP statistics.	**display rrpp statistics domain** *domain-id* [**ring** *ring-id*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear RRPP statistics.	**reset rrpp statistics domain** *domain-id* [**ring** *ring-id*]	Available in user view

RRPP configuration examples

Single ring configuration example

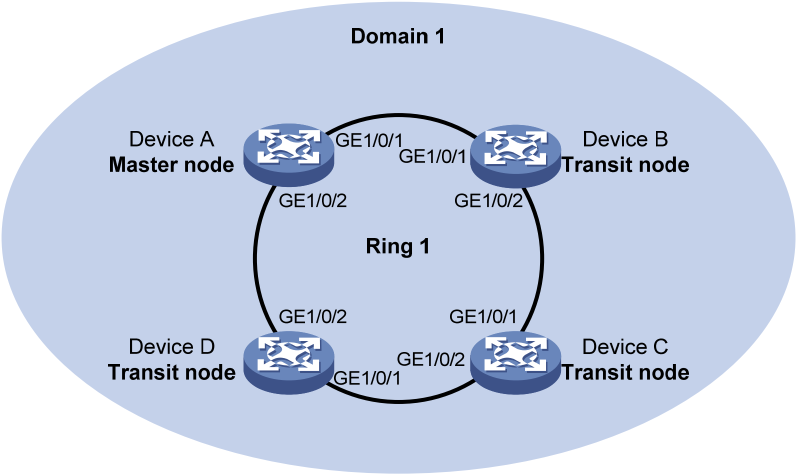
Networking requirements

As shown in Figure 18,

- Device A, Device B, Device C, and Device D form RRPP domain 1. Specify the primary control VLAN of RRPP domain 1 as VLAN 4092. RRPP domain 1 protects VLANs 1 through 30.
- Device A, Device B, Device C, and Device D form primary ring 1.

- Specify Device A as the master node of primary ring 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.
- Specify Device B, Device C, and Device D as the transit nodes of primary ring 1. Specify their GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

Figure 18 Network diagram



Configuration procedure

1. Configure Device A:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1 to 30
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo link-delay
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo link-delay
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceA] rrpp domain 1
[DeviceA-rrpp-domain1] control-vlan 4092
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceA] rrpp enable
```

2. Configure Device B:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo link-delay
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo link-delay
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceB] rrpp domain 1
[DeviceB-rrpp-domain1] control-vlan 4092
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device B as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
[DeviceB-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceB] rrpp enable
```

3. Configure Device C:

   The configuration on Device C is similar to that on Device B and is not shown here.

4. Configure Device D:

   The configuration on Device D is similar to that on Device B and is not shown here.

5. Verify the configuration:

   Use the **display** command to view RRPP configuration and operational information on each device.

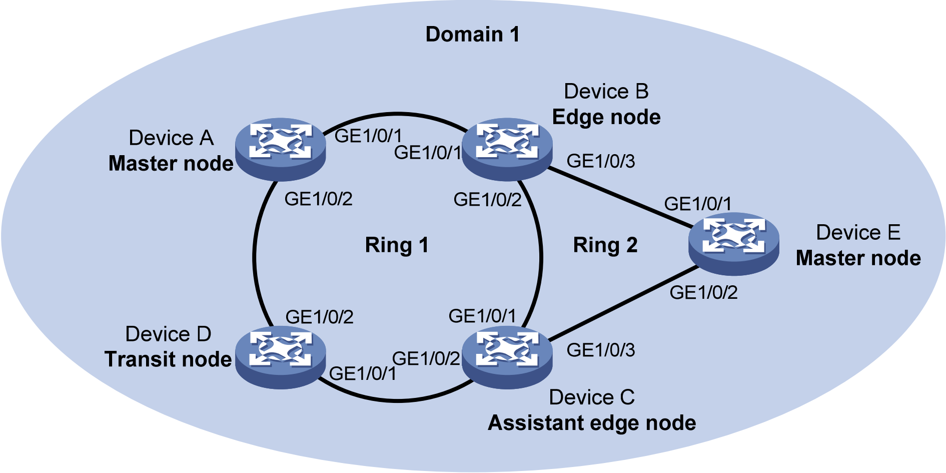
Intersecting ring configuration example

Networking requirements

As shown in Figure 19,

- Device A, Device B, Device C, Device D, and Device E form RRPP domain 1. VLAN 4092 is the primary control VLAN of RRPP domain 1, and RRPP domain 1 protects VLANs 1 through 30.
- Device A, Device B, Device C, and Device D form primary ring 1, and Device B, Device C and Device E form subring 2.
- Device A is the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 the secondary port.
- Device E is the master node of subring 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 the secondary port.
- Device B is the transit node of primary ring 1 and the edge node of subring 2, and GigabitEthernet 1/0/3 is the edge port.
- Device C is the transit node of primary ring 1 and the assistant-edge node of subring 1, and GigabitEthernet 1/0/3 is the edge port.
- Device D is the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 the secondary port.

Figure 19 Network diagram



Configuration procedure

1. Configure Device A:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1 to 30
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo link-delay
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo link-delay
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceA] rrpp domain 1
[DeviceA-rrpp-domain1] control-vlan 4092
```

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceA] rrpp enable
```

2. Configure Device B:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the three ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo link-delay
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo link-delay
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] undo link-delay
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] qos trust dot1p
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/3] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceB] rrpp domain 1
[DeviceB-rrpp-domain1] control-vlan 4092
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device B as a transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
```

# Configure Device B as the edge node of subring 2, with GigabitEthernet 1/0/3 as the edge port, and enable ring 2.

```
[DeviceB-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceB-rrpp-domain1] ring 2 enable
[DeviceB-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceB] rrpp enable
```

3. Configure Device C:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 30
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the three ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo link-delay
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] qos trust dot1p
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo link-delay
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] qos trust dot1p
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo link-delay
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] qos trust dot1p
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/3] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceC] rrpp domain 1
[DeviceC-rrpp-domain1] control-vlan 4092
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device C as a transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable
```

# Configure Device C as the assistant-edge node of subring 2, with GigabitEthernet 1/0/3 as the edge port, and enable ring 2.

```
[DeviceC-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet
1/0/3
[DeviceC-rrpp-domain1] ring 2 enable
[DeviceC-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceC] rrpp enable
```

4. Configure Device D:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 30
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo link-delay
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] qos trust dot1p
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo link-delay
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] qos trust dot1p
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceD] rrpp domain 1
[DeviceD-rrpp-domain1] control-vlan 4092
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device D as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
[DeviceD-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceD] rrpp enable
```

5. Configure Device E:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceE> system-view
[DeviceE] vlan 1 to 30
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 1 vlan 1 to 30
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo link-delay
[DeviceE-GigabitEthernet1/0/1] undo stp enable
[DeviceE-GigabitEthernet1/0/1] qos trust dot1p
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/1] quit
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo link-delay
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] qos trust dot1p
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceE] rrpp domain 1
[DeviceE-rrpp-domain1] control-vlan 4092
[DeviceE-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device E as the master node of subring 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 2.

```
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceE-rrpp-domain1] ring 2 enable
[DeviceE-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceE] rrpp enable
```

6. Verify the configuration:

   Use the **display** command to view RRPP configuration and operational information on each device.

Dual homed rings configuration example

Networking requirements

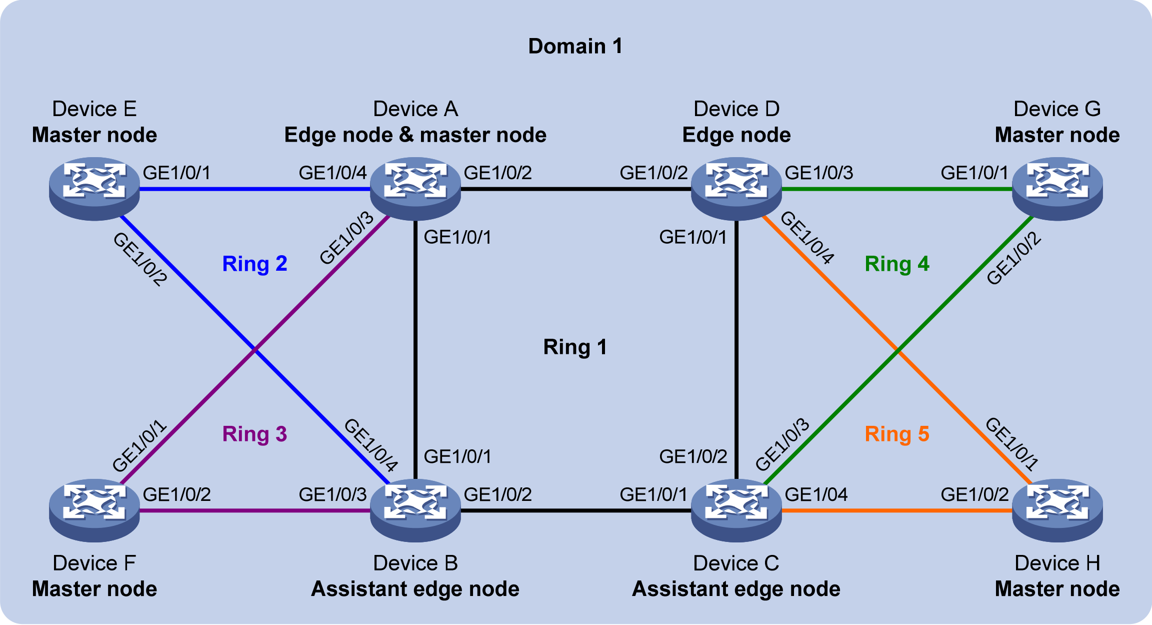
As shown in Figure 20,

- Device A through Device H form RRPP domain 1. Specify the primary control VLAN of RRPP domain 1 as VLAN 4092, and specify that RRPP domain 1 protects VLANs 1 through 30.
- Device A through Device D form primary ring 1. Device A, Device B, and Device E form subring 2. Device A, Device B, and Device F form subring 3. Device C, Device D, and Device G form subring 4. Device C, Device D, and Device H form subring 5.
- Specify Device A as the master node of primary ring 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Specify Device E as the master node of subring 2, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Specify Device F as the master node of subring 3, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Specify Device G as the master node of subring 4, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Specify Device H as the master node of subring 5, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.
- Specify Device A as the edge node of the connected subrings, its GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 as the edge ports. Specify Device D as the transit node of the primary ring and edge node of the connected subrings, its GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 as the edge ports. Specify Device B and Device C as the transit node of the primary ring and assistant-edge nodes of the connected subrings, their GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 as the edge ports.

NOTE:

Configure the primary and secondary ports on the master nodes properly to make sure that other protocols still work normally when data VLANs are denied by the secondary ports.

Figure 20 Network diagram



Configuration procedure

1. Configure Device A:

   # Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1 to 30
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

   # Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the four ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo link-delay
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo link-delay
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] quit
```

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] undo link-delay
[DeviceA-GigabitEthernet1/0/3] undo stp enable
[DeviceA-GigabitEthernet1/0/3] qos trust dot1p
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/3] quit
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] undo link-delay
[DeviceA-GigabitEthernet1/0/4] undo stp enable
[DeviceA-GigabitEthernet1/0/4] qos trust dot1p
[DeviceA-GigabitEthernet1/0/4] port link-type trunk
[DeviceA-GigabitEthernet1/0/4] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/4] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceA] rrpp domain 1
[DeviceA-rrpp-domain1] control-vlan 4092
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
```

# Configure Device A as the edge node of subring 2, with GigabitEthernet 1/0/4 as the edge port, and enable subring 2.

```
[DeviceA-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceA-rrpp-domain1] ring 2 enable
```

# Configure Device A as the edge node of subring 3, with GigabitEthernet 1/0/3 as the edge port, and enable subring 3.

```
[DeviceA-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceA-rrpp-domain1] ring 3 enable
[DeviceA-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceA] rrpp enable
```

2. Configure Device B:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4, disable the spanning tree feature, and set the trusted packet priority type

to 802.1p priority. Configure the four ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo link-delay
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo link-delay
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] undo link-delay
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] qos trust dot1p
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/3] quit
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] undo link-delay
[DeviceB-GigabitEthernet1/0/4] undo stp enable
[DeviceB-GigabitEthernet1/0/4] qos trust dot1p
[DeviceB-GigabitEthernet1/0/4] port link-type trunk
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/4] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceB] rrpp domain 1
[DeviceB-rrpp-domain1] control-vlan 4092
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device B as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
```

# Configure Device B as the assistant-edge node of subring 2, with GigabitEthernet 1/0/4 as the edge port, and enable subring 2.

```
[DeviceB-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet
1/0/4
[DeviceB-rrpp-domain1] ring 2 enable
```

# Configure Device B as the assistant-edge node of subring 3, with GigabitEthernet 1/0/3 as the edge port, and enable subring 3.

```
[DeviceB-rrpp-domain1] ring 3 node-mode assistant-edge edge-port gigabitethernet
1/0/3
[DeviceB-rrpp-domain1] ring 3 enable
[DeviceB-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceB] rrpp enable
```

3. Configure Device C:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 30
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the four ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo link-delay
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] qos trust dot1p
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo link-delay
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] qos trust dot1p
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo link-delay
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] qos trust dot1p
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/3] quit
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] undo link-delay
[DeviceC-GigabitEthernet1/0/4] undo stp enable
[DeviceC-GigabitEthernet1/0/4] qos trust dot1p
[DeviceC-GigabitEthernet1/0/4] port link-type trunk
[DeviceC-GigabitEthernet1/0/4] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/4] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceC] rrpp domain 1
[DeviceC-rrpp-domain1] control-vlan 4092
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device C as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable
```

# Configure Device C as the assistant-edge node of subring 4, with GigabitEthernet 1/0/3 as the edge port, and enable subring 4.

```
[DeviceC-rrpp-domain1] ring 4 node-mode assistant-edge edge-port gigabitethernet
1/0/3
[DeviceC-rrpp-domain1] ring 4 enable
```

# Configure Device C as the assistant-edge node of subring 5, with GigabitEthernet 1/0/4 as the edge port, and enable subring 5.

```
[DeviceC-rrpp-domain1] ring 5 node-mode assistant-edge edge-port gigabitethernet
1/0/4
[DeviceC-rrpp-domain1] ring 5 enable
[DeviceC-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceC] rrpp enable
```

4. Configure Device D:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 30
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the four ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo link-delay
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] qos trust dot1p
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo link-delay
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] qos trust dot1p
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
```

```
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/2] quit
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] undo link-delay
[DeviceD-GigabitEthernet1/0/3] undo stp enable
[DeviceD-GigabitEthernet1/0/3] qos trust dot1p
[DeviceD-GigabitEthernet1/0/3] port link-type trunk
[DeviceD-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/3] quit
[DeviceD] interface gigabitethernet 1/0/4
[DeviceD-GigabitEthernet1/0/4] undo link-delay
[DeviceD-GigabitEthernet1/0/4] undo stp enable
[DeviceD-GigabitEthernet1/0/4] qos trust dot1p
[DeviceD-GigabitEthernet1/0/4] port link-type trunk
[DeviceD-GigabitEthernet1/0/4] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/4] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceD] rrpp domain 1
[DeviceD-rrpp-domain1] control-vlan 4092
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device D as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
```

# Configure Device D as the edge node of subring 4, with GigabitEthernet 1/0/3 as the edge port, and enable subring 4.

```
[DeviceD-rrpp-domain1] ring 4 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceD-rrpp-domain1] ring 4 enable
```

# Configure Device D as the edge node of subring 5, with GigabitEthernet 1/0/4 as the edge port, and enable subring 5.

```
[DeviceD-rrpp-domain1] ring 5 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceD-rrpp-domain1] ring 5 enable
[DeviceD-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceD] rrpp enable
```

5. Configure Device E:

   # Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceE> system-view
[DeviceE] vlan 1 to 30
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 1 vlan 1 to 30
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo link-delay
[DeviceE-GigabitEthernet1/0/1] undo stp enable
[DeviceE-GigabitEthernet1/0/1] qos trust dot1p
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/1] quit
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo link-delay
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] qos trust dot1p
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceE] rrpp domain 1
[DeviceE-rrpp-domain1] control-vlan 4092
[DeviceE-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device E as the master node of subring 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable subring 2.

```
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceE-rrpp-domain1] ring 2 enable
[DeviceE-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceE] rrpp enable
```

6. Configure Device F:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceF> system-view
[DeviceF] vlan 1 to 30
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 1 to 30
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] undo link-delay
[DeviceF-GigabitEthernet1/0/1] undo stp enable
[DeviceF-GigabitEthernet1/0/1] qos trust dot1p
```

```
[DeviceF-GigabitEthernet1/0/1] port link-type trunk
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceF-GigabitEthernet1/0/1] quit
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] undo link-delay
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] qos trust dot1p
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceF-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceF] rrpp domain 1
[DeviceF-rrpp-domain1] control-vlan 4092
[DeviceF-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device F as the master node of subring 3, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable subring 3.

```
[DeviceF-rrpp-domain1] ring 3 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceF-rrpp-domain1] ring 3 enable
[DeviceF-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceF] rrpp enable
```

7. Configure Device G:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceG> system-view
[DeviceG] vlan 1 to 30
[DeviceG] stp region-configuration
[DeviceG-mst-region] instance 1 vlan 1 to 30
[DeviceG-mst-region] active region-configuration
[DeviceG-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceG] interface gigabitethernet 1/0/1
[DeviceG-GigabitEthernet1/0/1] undo link-delay
[DeviceG-GigabitEthernet1/0/1] undo stp enable
[DeviceG-GigabitEthernet1/0/1] qos trust dot1p
[DeviceG-GigabitEthernet1/0/1] port link-type trunk
[DeviceG-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceG-GigabitEthernet1/0/1] quit
[DeviceG] interface gigabitethernet 1/0/2
[DeviceG-GigabitEthernet1/0/2] undo link-delay
[DeviceG-GigabitEthernet1/0/2] undo stp enable
[DeviceG-GigabitEthernet1/0/2] qos trust dot1p
[DeviceG-GigabitEthernet1/0/2] port link-type trunk
```

```
[DeviceG-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceG-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceG] rrpp domain 1
[DeviceG-rrpp-domain1] control-vlan 4092
[DeviceG-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device G as the master node of subring 4, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable subring 4.

```
[DeviceG-rrpp-domain1] ring 4 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceG-rrpp-domain1] ring 4 enable
[DeviceG-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceG] rrpp enable
```

8. Configure Device H:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceH> system-view
[DeviceH] vlan 1 to 30
[DeviceH] stp region-configuration
[DeviceH-mst-region] instance 1 vlan 1 to 30
[DeviceH-mst-region] active region-configuration
[DeviceH-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceH] interface gigabitethernet 1/0/1
[DeviceH-GigabitEthernet1/0/1] undo link-delay
[DeviceH-GigabitEthernet1/0/1] undo stp enable
[DeviceH-GigabitEthernet1/0/1] qos trust dot1p
[DeviceH-GigabitEthernet1/0/1] port link-type trunk
[DeviceH-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceH-GigabitEthernet1/0/1] quit
[DeviceH] interface gigabitethernet 1/0/2
[DeviceH-GigabitEthernet1/0/2] undo link-delay
[DeviceH-GigabitEthernet1/0/2] undo stp enable
[DeviceH-GigabitEthernet1/0/2] qos trust dot1p
[DeviceH-GigabitEthernet1/0/2] port link-type trunk
[DeviceH-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceH-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1. Configure VLAN 4092 as the primary control VLAN of RRPP domain 1, and configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceH] rrpp domain 1
[DeviceH-rrpp-domain1] control-vlan 4092
[DeviceH-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device H as the master node of subring 5, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable subring 5.

```
[DeviceH-rrpp-domain1] ring 5 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceH-rrpp-domain1] ring 5 enable
[DeviceH-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceH] rrpp enable
```

9. Verify the configuration:

   Use the **display** command to view RRPP configuration and operational information on each device.

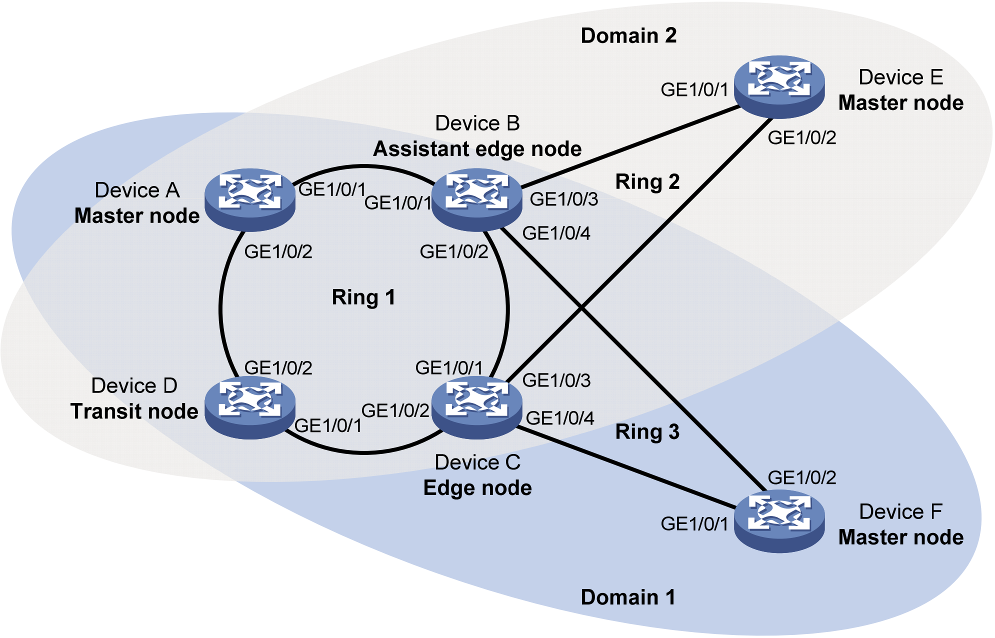
Intersecting-ring load balancing configuration example

Networking requirements

As shown in Figure 21,

- Device A, Device B, Device C, Device D, and Device F form RRPP domain 1, and VLAN 100 is the primary control VLAN of the RRPP domain. Device A is the master node of the primary ring, Ring 1; Device D is the transit node of Ring 1; Device F is the master node of the subring Ring 3; Device C is the edge node of the subring Ring 3; Device B is the assistant-edge node of the subring Ring 3.
- Device A, Device B, Device C, Device D, and Device E form RRPP domain 2, and VLAN 105 is the primary control VLAN of the RRPP domain. Device A is the master node of the primary ring, Ring 1; Device D is the transit node of Ring 1; Device E is the master node of the subring Ring 2; Device C is the edge node of the subring Ring 2; Device B is the assistant-edge node of the subring Ring 2.
- Specify VLAN 1 as the protected VLAN of domain 1 and VLAN 2 the protected VLAN of domain 2. You can implement VLAN-based load balancing on Ring 1.
- Because the edge node and assistant-edge node of Ring 2 are the same as those of Ring 3 and the two subrings have the same SRPTs, you can add Ring 2 and Ring 3 to the RRPP ring group to reduce Edge-Hello traffic.

Figure 21 Network diagram



Configuration procedure

1. Configure Device A:

# Create VLANs 1 and 2, map VLAN 1 to MSTI 1 and VLAN 2 to MSTI 2, and activate MST region configuration.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 2
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1
[DeviceA-mst-region] instance 2 vlan 2
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, and assign them to VLAN 1 and VLAN 2.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo link-delay
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] qos trust dot1p
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 2
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo link-delay
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] qos trust dot1p
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 2
```

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

# Create RRPP domain 1. Configure VLAN 100 as the primary control VLAN of RRPP domain 1, and configure the VLAN mapped to MSTI 1 as the protected VLAN of RRPP domain 1.

```
[DeviceA] rrpp domain 1
[DeviceA-rrpp-domain1] control-vlan 100
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

# Create RRPP domain 2, configure VLAN 105 as the primary control VLAN of RRPP domain 2, and configure the VLAN mapped to MSTI 2 as the protected VLAN of RRPP domain 2.

```
[DeviceA] rrpp domain 2
[DeviceA-rrpp-domain2] control-vlan 105
[DeviceA-rrpp-domain2] protected-vlan reference-instance 2
```

# Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/2 as the master port and GigabitEthernet 1/0/1 as the secondary port, and enable ring 1.

```
[DeviceA-rrpp-domain2] ring 1 node-mode master primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 0
[DeviceA-rrpp-domain2] ring 1 enable
[DeviceA-rrpp-domain2] quit
```

# Enable RRPP.

```
[DeviceA] rrpp enable
```

2. Configure Device B:

# Create VLANs 1 and 2, map VLAN 1 to MSTI 1 and VLAN 2 to MSTI 2, and activate MST region configuration.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 2
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1
[DeviceB-mst-region] instance 2 vlan 2
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, and assign them to VLAN 1 and VLAN 2.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo link-delay
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] qos trust dot1p
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 2
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] undo link-delay
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] qos trust dot1p
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 2
[DeviceB-GigabitEthernet1/0/2] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/3, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the port as a trunk port, and assign it to VLAN 2.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] undo link-delay
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] qos trust dot1p
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 2
[DeviceB-GigabitEthernet1/0/3] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/4, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the port as a trunk port, and assign it to VLAN 1.

```
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] undo link-delay
[DeviceB-GigabitEthernet1/0/4] undo stp enable
[DeviceB-GigabitEthernet1/0/4] qos trust dot1p
[DeviceB-GigabitEthernet1/0/4] port link-type trunk
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/4] quit
```

# Create RRPP domain 1. Configure VLAN 100 as the primary control VLAN of RRPP domain 1, and configure the VLAN mapped to MSTI 1 as the protected VLAN of RRPP domain 1.

```
[DeviceB] rrpp domain 1
[DeviceB-rrpp-domain1] control-vlan 100
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device B as a transit node of primary ring 1 in RRPP domain 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
```

# Configure Device B as the assistant-edge node of subring 3 in RRPP domain 1, with GigabitEthernet 1/0/4 as the edge port, and enable subring 3.

```
[DeviceB-rrpp-domain1] ring 3 node-mode assistant-edge edge-port gigabitethernet
1/0/4
[DeviceB-rrpp-domain1] ring 3 enable
[DeviceB-rrpp-domain1] quit
```

# Create RRPP domain 2. Configure VLAN 105 as the primary control VLAN of RRPP domain 2, and configure the VLAN mapped to MSTI 2 as the protected VLAN of RRPP domain 2.

```
 [DeviceB] rrpp domain 2
[DeviceB-rrpp-domain2] control-vlan 105
[DeviceB-rrpp-domain2] protected-vlan reference-instance 2
```

# Configure Device B as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceB-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain2] ring 1 enable
```

# Configure Device B as the assistant-edge node of subring 2 in RRPP domain 2, with GigabitEthernet 1/0/3 as the edge port, and enable subring 2.

```
[DeviceB-rrpp-domain2] ring 2 node-mode assistant-edge edge-port gigabitethernet
1/0/3
[DeviceB-rrpp-domain2] ring 2 enable
[DeviceC-rrpp-domain2] quit
```

# Enable RRPP.

```
[DeviceB] rrpp enable
```

3. Configure Device C:

# Create VLANs 1 and 2, map VLAN 1 to MSTI 1 and VLAN 2 to MSTI 2, and activate MST region configuration.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 2
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1
[DeviceC-mst-region] instance 2 vlan 2
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, and assign them to VLAN 1 and VLAN 2.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo link-delay
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] qos trust dot1p
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 2
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo link-delay
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] qos trust dot1p
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 2
[DeviceC-GigabitEthernet1/0/2] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/3, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the port as a trunk port, remove it from VLAN 1, assign it to VLAN 2, and configure VLAN 2 as its default VLAN.

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo link-delay
[DeviceC-GigabitEthernet1/0/3] undo stp enable
```

```
[DeviceC-GigabitEthernet1/0/3] qos trust dot1p
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 2
[DeviceC-GigabitEthernet1/0/3] port trunk pvid vlan 2
[DeviceC-GigabitEthernet1/0/3] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/4, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the port as a trunk port, and assign it to VLAN 1.

```
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] undo link-delay
[DeviceC-GigabitEthernet1/0/4] undo stp enable
[DeviceC-GigabitEthernet1/0/4] qos trust dot1p
[DeviceC-GigabitEthernet1/0/4] port link-type trunk
[DeviceC-GigabitEthernet1/0/4] port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/4] quit
```

# Create RRPP domain 1. Configure VLAN 100 as the primary control VLAN of RRPP domain 1, and configure the VLAN mapped to MSTI 1 as the protected VLAN of RRPP domain 1.

```
[DeviceC] rrpp domain 1
[DeviceC-rrpp-domain1] control-vlan 100
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device C as the transit node of primary ring 1 in RRPP domain 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable
```

# Configure Device C as the edge node of subring 3 in RRPP domain 1, with GigabitEthernet 1/0/4 as the edge port, and enable subring 3.

```
[DeviceC-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceC-rrpp-domain1] ring 3 enable
[DeviceC-rrpp-domain1] quit
```

# Create RRPP domain 2. Configure VLAN 105 as the primary control VLAN of RRPP domain 2, and configure the VLAN mapped to MSTI 2 as the protected VLAN of RRPP domain 2.

```
[DeviceC] rrpp domain 2
[DeviceC-rrpp-domain2] control-vlan 105
[DeviceC-rrpp-domain2] protected-vlan reference-instance 2
```

# Configure Device C as the transit node of primary ring 1 in RRPP domain 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceC-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain2] ring 1 enable
```

# Configure Device C as the edge node of subring 2 in RRPP domain 2, with GigabitEthernet 1/0/3 as the edge port, and enable subring 2.

```
[DeviceC-rrpp-domain2] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain2] ring 2 enable
[DeviceC-rrpp-domain2] quit
```

# Enable RRPP.

```
[DeviceC] rrpp enable
```

4. Configure Device D:

# Create VLANs 1 and 2, map VLAN 1 to MSTI 1 and VLAN 2 to MSTI 2, and activate MST region configuration.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 2
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1
[DeviceD-mst-region] instance 2 vlan 2
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, and assign them to VLAN 1 and VLAN 2.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo link-delay
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] qos trust dot1p
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 2
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo link-delay
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] qos trust dot1p
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 2
[DeviceD-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1. Configure VLAN 100 as the primary control VLAN of RRPP domain 1, and configure the VLAN mapped to MSTI 1 as the protected VLAN of RRPP domain 1.

```
[DeviceD] rrpp domain 1
[DeviceD-rrpp-domain1] control-vlan 100
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device D as the transit node of primary ring 1 in RRPP domain 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
[DeviceD-rrpp-domain1] quit
```

# Create RRPP domain 2. Configure VLAN 105 as the primary control VLAN of RPPP domain 2, and configure the VLAN mapped to MSTI 2 as the protected VLAN of RRPP domain 2.

```
[DeviceD] rrpp domain 2
[DeviceD-rrpp-domain2] control-vlan 105
[DeviceD-rrpp-domain2] protected-vlan reference-instance 2
```

# Configure Device D as the transit node of primary ring 1 in RRPP domain 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable ring 1.

```
[DeviceD-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain2] ring 1 enable
[DeviceD-rrpp-domain2] quit
```

# Enable RRPP.

```
[DeviceD] rrpp enable
```

5. Configure Device E:

# Create VLAN 2, map VLAN 2 to MSTI 2, and activate MST region configuration.

```
<DeviceE> system-view
[DeviceE] vlan 2
[DeviceE-vlan2] quit
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 2 vlan 2
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, remove them from VLAN 1, assign them to VLAN 2, and configure VLAN 2 as their default VLAN.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo link-delay
[DeviceE-GigabitEthernet1/0/1] undo stp enable
[DeviceE-GigabitEthernet1/0/1] qos trust dot1p
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 2
[DeviceE-GigabitEthernet1/0/1] port trunk pvid vlan 2
[DeviceE-GigabitEthernet1/0/1] quit
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo link-delay
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] qos trust dot1p
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 2
[DeviceE-GigabitEthernet1/0/2] port trunk pvid vlan 2
[DeviceE-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 2. Configure VLAN 105 as the primary control VLAN, and configure the VLAN mapped to MSTI 2 as the protected VLAN.

```
[DeviceE] rrpp domain 2
[DeviceE-rrpp-domain2] control-vlan 105
[DeviceE-rrpp-domain2] protected-vlan reference-instance 2
```

# Configure Device E as the master mode of subring 2 in RRPP domain 2, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port, and enable ring 2.

```
[DeviceE-rrpp-domain2] ring 2 node-mode master primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 1
[DeviceE-rrpp-domain2] ring 2 enable
[DeviceE-rrpp-domain2] quit
```

# Enable RRPP.

```
[DeviceE] rrpp enable
```

6. Configure Device F:

# Create VLAN 1, map VLAN 1 to MSTI 1, and activate MST region configuration.

```
<DeviceF> system-view
[DeviceF] vlan 1
[DeviceF-vlan1] quit
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 1
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit
```

# Cancel the physical state change suppression interval setting on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature, and set the trusted packet priority type to 802.1p priority. Configure the two ports as trunk ports, and assign them to VLAN 1.

```
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] undo link-delay
[DeviceF-GigabitEthernet1/0/1] undo stp enable
[DeviceF-GigabitEthernet1/0/1] qos trust dot1p
[DeviceF-GigabitEthernet1/0/1] port link-type trunk
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 1
[DeviceF-GigabitEthernet1/0/1] quit
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] undo link-delay
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] qos trust dot1p
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 1
[DeviceF-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1. Configure VLAN 100 as the primary control VLAN, and configure the VLAN mapped to MSTI 1 as the protected VLAN.

```
[DeviceF] rrpp domain 1
[DeviceF-rrpp-domain1] control-vlan 100
[DeviceF-rrpp-domain1] protected-vlan reference-instance 1
```

# Configure Device F as the master node of subring 3 in RRPP domain 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port, and enable subring 3.

```
[DeviceF-rrpp-domain1] ring 3 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceF-rrpp-domain1] ring 3 enable
[DeviceF-rrpp-domain1] quit
```

# Enable RRPP.

```
[DeviceF] rrpp enable
```

7. RRPP ring group configurations on Device B and Device C after the configurations.

# Create RRPP ring group 1 on Device B. Add subrings 2 and 3 to the RRPP ring group.

```
[DeviceB] rrpp ring-group 1
[DeviceB-rrpp-ring-group1] domain 2 ring 2
[DeviceB-rrpp-ring-group1] domain 1 ring 3
```

# Create RRPP ring group 1 on Device C, and add subrings 2 and 3 to the RRPP ring group.

```
[DeviceC] rrpp ring-group 1
[DeviceC-rrpp-ring-group1] domain 2 ring 2
[DeviceC-rrpp-ring-group1] domain 1 ring 3
```

8. Verify the configuration:

   Use the **display** command to view RRPP configuration and operational information on each device.

Troubleshooting

Symptom

When the link state is normal, the master node cannot receive Hello packets, and the master node unblocks the secondary port.

Analysis

The reasons may be:

- RRPP is not enabled on some nodes in the RRPP ring.
- The domain ID or primary control VLAN ID is not the same for the nodes in the same RRPP ring.
- Some ports are abnormal.

Solution

- Use the **display rrpp brief** command to examine whether RRPP is enabled for all nodes. If it is not, use the **rrpp enable** command and the **ring enable** command to enable RRPP and RRPP rings for all nodes.
- Use the **display rrpp brief** command to examine whether the domain ID and primary control VLAN ID are the same for all nodes. If they are not, set the same domain ID and primary control VLAN ID for the nodes.
- Use the **display rrpp verbose** command to examine the link state of each port in each ring.
- Use the **debugging rrpp** command on each node to examine whether a port receives or transmits Hello packets. If it does not, Hello packets are lost.

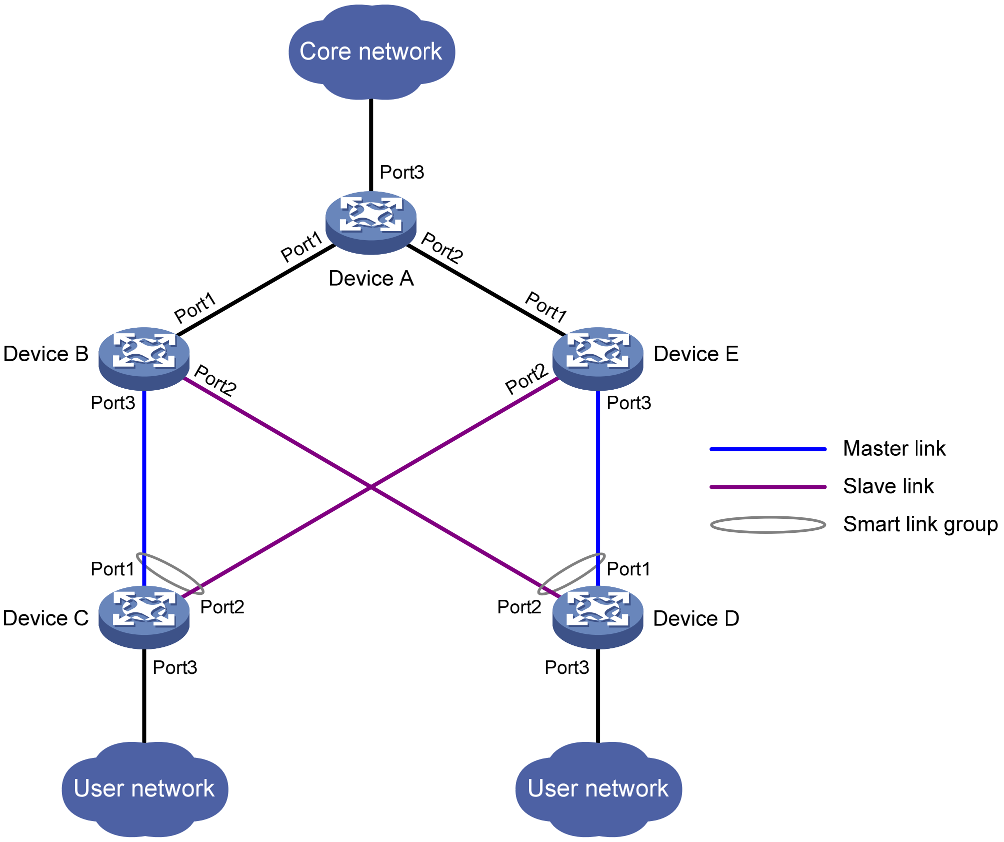
Configuring Smart Link

Smart Link overview

Background

To avoid single-point failures and guarantee network reliability, downstream devices are usually dual-homed to upstream devices, as shown in Figure 22.

Figure 22 Diagram for a dual uplink network



To remove network loops on a dual-homed network, you can use a spanning tree protocol or the Rapid Ring Protection Protocol (RRPP). The problem with STP, however, is that STP convergence time is long, which makes it not suitable for users who have high demand on convergence speed. RRPP can meet users' demand on convergence speed, but it involves complicated networking and configurations and is mainly used in ring-shaped networks.

For more information about STP and RRPP, see *Layer 2—LAN Switching Configuration Guide* and "Configuring RRPP."

Smart Link is a feature developed to address the slow convergence issue with STP. It provides link redundancy as well as fast convergence in a dual uplink network, allowing the backup link to take over quickly when the primary link fails. To sum up, Smart Link has the following features:

- Dedicated to dual uplink networks
- Subsecond convergence
- Easy to configure

Terminology

Smart link group

A smart link group consists of only two member ports: the master and the slave ports. At a time, only one port is active for forwarding, and the other port is blocked and in standby state. When link failure occurs on the active port due to port shutdown or presence of unidirectional link, the standby port becomes active to take over and the original active port transits to the blocked state.

As shown in Figure 22, Port1 and Port2 of Device C and Port1 and Port2 of Device D each form a smart link group, with Port1 being active and Port2 being standby.

Master/slave port

Master port and slave port are two port roles in a smart link group. When both ports in a smart link group are up, the master port preferentially transits to the forwarding state, and the slave port stays in standby state. Once the master port fails, the slave port takes over to forward traffic. As shown in Figure 22, you can configure Port1 of Device C and Port1 of Device D as master ports, and Port2 of Device C and Port2 of Device D slave ports.

Master/slave link

The link that connects the master port in a smart link group is the master link. The link that connects the slave port is the slave link.

Flush message

Flush messages are used by a smart link group to notify other devices to refresh their MAC address forwarding entries and ARP/ND entries when link switchover occurs in the smart link group. Flush messages are common multicast data packets, and will be dropped by a blocked receiving port.

Protected VLAN

A smart link group controls the forwarding state of some data VLANs (protected VLANs). Different smart link groups on a port control different protected VLANs. The state of the port in a protected VLAN is determined by the state of the port in the smart link group.

Transmit control VLAN

The transmit control VLAN is used for transmitting flush messages. When link switchover occurs, the devices (such as Device C and Device D in Figure 22) broadcast flush messages within the transmit control VLAN.

Receive control VLAN

The receive control VLAN is used for receiving and processing flush messages. When link switchover occurs, the devices (such as Device A, Device B, and Device E in Figure 22) receive and process flush messages in the receive control VLAN and refresh their MAC address forwarding entries and ARP/ND entries.

How Smart Link works

Link backup mechanism

As shown in Figure 22, the link on Port1 of Device C is the master link, and the link on Port2 of Device C is the slave link. Typically, Port1 is in forwarding state, and Port2 is in standby state. When the master link fails, Port2 takes over to forward traffic and Port1 is blocked and placed in standby state.

NOTE:

When a port switches to the forwarding state, the system outputs log information to notify the user of the port state change.

Topology change mechanism

Because link switchover can outdate the MAC address forwarding entries and ARP/ND entries on all devices, you need a forwarding entry update mechanism to ensure proper transmission. By far, the following two update mechanisms are provided:

- Uplink traffic-triggered MAC address learning, where update is triggered by uplink traffic. This mechanism is applicable to environments with devices not supporting Smart Link, including devices of other vendors'.
- Flush update where a Smart Link-enabled device updates its information by transmitting flush messages over the backup link to its upstream devices. This mechanism requires the upstream devices to be capable of recognizing Smart Link flush messages to update its MAC address forwarding entries and ARP/ND entries.

Role preemption mechanism

As shown in Figure 22, the link on Port1 of Device C is the master link, and the link on Port2 of Device C is the slave link. Once the master link fails, Port1 is automatically blocked and placed in standby state, and Port2 takes over to forward traffic. When the master link recovers, one of the following occurs:

- If the smart link group is not configured with role preemption, to keep traffic forwarding stable, Port1 that has been blocked due to link failure does not immediately take over to forward traffic. Rather, it stays blocked until the next link switchover.
- If the smart link group is configured with role preemption, Port1 takes over to forward traffic as soon as its link recovers, and Port2 is automatically blocked and placed in standby state.

Load sharing mechanism

A ring network may carry traffic of multiple VLANs. Smart Link can forward traffic of different VLANs in different smart link groups, implementing load sharing.

To implement load sharing, you can assign a port to multiple smart link groups (each configured with different protected VLANs), making sure that the state of the port is different in these smart link groups. In this way, traffic of different VLANs can be forwarded along different paths.

You can configure protected VLANs for a smart link group by referencing Multiple Spanning Tree Instances (MSTIs).

Smart Link collaboration mechanisms

Collaboration between Smart Link and Monitor Link

Smart Link cannot sense by itself when faults occur on the uplink of the upstream devices, or when faults are cleared. To monitor the uplink status of the upstream devices, you can configure the Monitor Link function to monitor the uplink ports of the upstream devices. Monitor Link adapts the up/down state of downlink ports to the up/down state of uplink ports, triggering Smart Link to perform link switchover on the downstream device.

For more information about Monitor Link, see "Configuring Monitor Link."

Collaboration between Smart Link and CC of CFD

Smart Link cannot sense by itself when faults (for example, unidirectional link, misconnected fibers, and packet loss) occur on the intermediate devices or network paths, or when faults are cleared. To check the link status, Smart Link ports must use link detection protocols. When a fault is detected or cleared, the link detection protocols inform Smart Link to switch over the links.

With the collaboration between Smart Link and the Continuity Check (CC) function of Connectivity Fault Detection (CFD) configured, CFD notifies the ports of fault detection events on the basis of detection VLANs and detection ports. A port responds to a continuity check event only when the control VLAN of the smart link group to which it belongs matches the detection VLAN.

For more information about the CC function of CFD, see "Configuring CFD."

Smart Link configuration task list

A smart link device is a device that supports Smart Link and is configured with a smart link group and a transmit control VLAN for flush message transmission. Device C and Device D in Figure 22 are two examples of smart link devices.

An associated device is a device that supports Smart Link and receives flush messages sent from the specified control VLAN. Device A, Device B, and Device E in Figure 22 are examples of associated devices.

Complete the following tasks to configure Smart Link:

Task		Remarks
Configuring a Smart Link device	Configuring protected VLANs for a smart link group	Required
	Configuring member ports for a smart link group	Required
	Configuring role preemption for a smart link group	Optional
	Enabling the sending of flush messages	Optional
	Configuring the collaboration between Smart Link and CC of CFD	Optional
Configuring an associated device	Enabling the receiving of flush messages	Required

Configuring a Smart Link device

Configuration prerequisites

- Before configuring a port as a smart link group member, shut down the port to prevent loops. You can bring up the port only after completing the smart link group configuration.

- Disable the spanning tree feature and RRPP on the ports that you want to add to the smart link group, and make sure the ports are not member ports of any aggregation group or service loopback group.

NOTE:

A loop may occur on the network during the time when the spanning tree feature is disabled but Smart Link has not yet taken effect on a port.

Configuring protected VLANs for a smart link group

You can configure protected VLANs for a smart link group by referencing MSTIs. Before configuring the protected VLANs, configure the mappings between MSTIs and the VLANs to be protected. (In PVST mode, the system automatically maps VLANs to MSTIs.) For more information about MSTI and PVST, see *Layer 2—LAN Switching Configuration Guide*.

To configure the protected VLANs for a smart link group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter MST region view.	**stp region-configuration**	Not required in PVST mode. For more information about the command, see *Layer 2—LAN Switching Command Reference*.
3. Configure the VLAN-to-instance mapping table.	Approach 1: **instance** *instance-id* **vlan** *vlan-list* Approach 2: **vlan-mapping modulo** *modulo*	Optional. Use either approach. All VLANs in an MST region are mapped to CIST (MSTI 0) by default. Not required in PVST mode. For more information about the commands, see *Layer 2—LAN Switching Command Reference*.
4. Activate MST region configuration manually.	**active region-configuration**	Not required in PVST mode. For more information about the command, see *Layer 2—LAN Switching Command Reference*.
5. Display the currently activated configuration information of the MST region.	**display stp region-configuration** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Optional. Available in any view. You can view the VLANs mapped to the MSTIs. For more information about the command, see *Layer 2—LAN Switching Command Reference*.
6. Return to system view.	**quit**	Not required in PVST mode.
7. Create a smart link group, and enter smart link group view.	**smart-link group** *group-id*	N/A

Step	Command	Remarks
8. Configure protected VLANs for the smart link group.	**protected-vlan reference-instance** *instance-id-list*	By default, no protected VLAN is configured for a smart link group.

Configuring member ports for a smart link group

You can configure member ports for a smart link group either in smart link group view or in interface view. The configurations made in these two views have the same effect.

In smart link group view

To configure member ports for a smart link group in smart link group view:

Step	Command
1. Enter system view.	**system-view**
2. Create a smart link group, and enter smart link group view.	**smart-link group** *group-id*
3. Configure member ports for a smart link group.	**port** *interface-type interface-number* { **master** | **slave** }

In interface view

To configure member ports for a smart link group in interface view:

Step	Command
1. Enter system view.	**system-view**
2. Enter Layer 2 Ethernet interface view or layer 2 aggregate interface view.	**interface** *interface-type interface-number*
3. Configure member ports for a smart link group.	**port smart-link group** *group-id* { **master** | **slave** }

Configuring role preemption for a smart link group

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a smart link group, and enter smart link group view.	**smart-link group** *group-id*	N/A
3. Enable role preemption.	**preemption mode role**	By default, the device works in the non-preemption mode.
4. Configure the preemption delay.	**preemption delay** *delay-time*	Optional. 1 second by default.

NOTE:

The preemption delay configuration takes effect only after role preemption is enabled.

Enabling the sending of flush messages

The control VLAN configured for a smart link group must be different from that configured for any other smart link group.

Make sure the configured control VLAN already exists, and assign the smart link group member ports to the control VLAN.

The control VLAN of a smart link group should also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent properly.

To enable the sending of flush messages:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a smart link group, and enter smart link group view.	**smart-link group** *group-id*	N/A
3. Enable flush update in the specified control VLAN.	**flush enable** [**control-vlan** *vlan-id*]	Optional. By default, flush update is enabled, and VLAN 1 is the control VLAN.

Configuring the collaboration between Smart Link and CC of CFD

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the collaboration between Smart Link and the CC function of CFD on the port.	**port smart-link group** *group-id* **track cfd cc**	Optional. By default, the collaboration between Smart Link and the CC function of CFD is not configured.

NOTE:

When configuring the collaboration between Smart Link and the CC function of CFD on a smart link member port, make sure that the control VLAN of the smart link group to which the port belongs matches the detection VLAN of the CC function of CFD.

Configuring an associated device

Configuration prerequisites

Disable the spanning tree feature on the associated device's ports that connect to the member ports of the smart link group; otherwise, the ports will discard flush messages when they are not in the forwarding state in case of a topology change.

Enabling the receiving of flush messages

You do not need to enable all ports on the associated devices to receive flush messages sent from the transmit control VLAN; you only need to enable those on the master and slave links between the smart link device and the destination device.

Configuration guidelines

- Configure all the control VLANs to receive flush messages.
- If no control VLAN is specified for processing flush messages, the device forwards the received flush messages without processing them.
- Make sure the receive control VLAN is the same as the transmit control VLAN configured on the smart link device. If they are not the same, the associated device will forward the received flush messages directly without any processing.
- Do not remove the control VLANs. Otherwise, flush messages cannot be sent properly.
- Make sure the control VLANs are existing VLANs, and assign the ports capable of receiving flush messages to the control VLANs.

Configuration procedure

To enable the receiving of flush messages:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the control VLANs for receiving flush messages.	**smart-link flush enable** [**control-vlan** *vlan-id-list*]	By default, no control VLAN exists for receiving flush messages.

Displaying and maintaining Smart Link

Task	Command	Remarks
Display smart link group information.	**display smart-link group** { *group-id* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display information about the received flush messages.	**display smart-link flush** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Task	Command	Remarks
Clear the statistics about flush messages.	**reset smart-link statistics**	Available in user view

Smart Link configuration examples

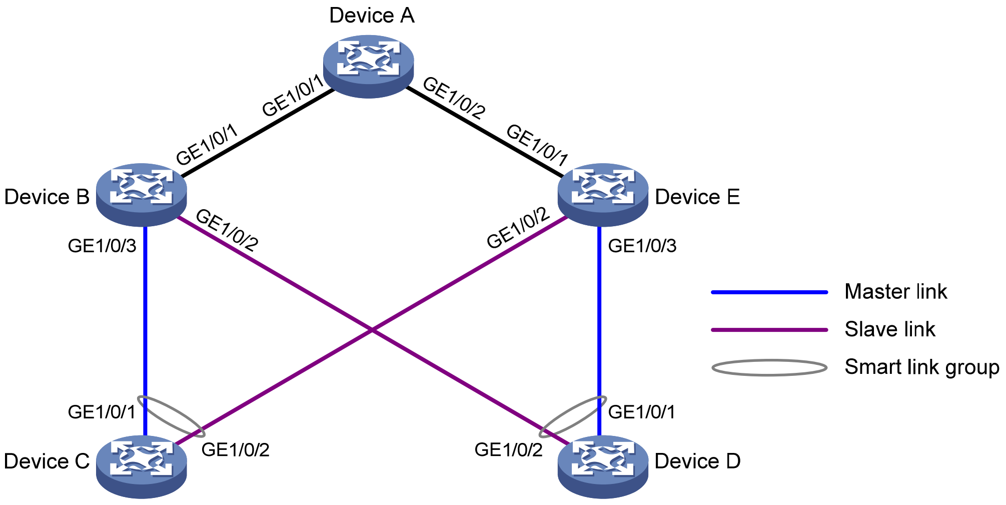
Single smart link group configuration example

Network requirements

As shown in Figure 23, Device C and Device D are smart link devices, and Device A, Device B, and Device E are associated devices. Traffic of VLANs 1 through 30 on Device C and Device D are dually uplinked to Device A.

Configure Smart Link on Device C and Device D for dual uplink backup.

Figure 23 Network diagram



Configuration procedure

1. Configure Device C:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 30
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

# Shut down GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 separately, configure them as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
```

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
```

# Create smart link group 1, and configure all VLANs mapped to MSTI 1 as the protected VLANs.

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

# Configure GigabitEthernet 1/0/1 as the master port and GigabitEthernet 1/0/2 as the slave port for smart link group 1.

```
[DeviceC-smlk-group1] port gigabitethernet1/0/1 master
[DeviceC-smlk-group1] port gigabitethernet1/0/2 slave
```

# Enable flush message sending in smart link group 1, and configure VLAN 10 as the transmit control VLAN.

```
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit
```

# Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 again.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

2. Configure Device D:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 30
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

# Shut down GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 separately, configure them as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] shutdown
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
```

```
[DeviceD-GigabitEthernet1/0/2] shutdown
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/2] quit
```

# Create smart link group 1, and configure all VLANs mapped to MSTI 1 as the protected VLANs.

```
[DeviceD] smart-link group 1
[DeviceD-smlk-group1] protected-vlan reference-instance 1
```

# Configure GigabitEthernet 1/0/1 as the master port and GigabitEthernet 1/0/2 as the slave port for smart link group 1.

```
[DeviceD-smlk-group1] port gigabitethernet1/0/1 master
[DeviceD-smlk-group1] port gigabitethernet1/0/2 slave
```

# Enable flush message sending in smart link group 1, and configure VLAN 20 as the transmit control VLAN.

```
[DeviceD-smlk-group1] flush enable control-vlan 20
[DeviceD-smlk-group1] quit
```

# Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 again.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] quit
```

3. Configure Device B:

# Create VLANs 1 through 30.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
```

# Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 1 through 30. Enable flush message receiving on it, and configure VLAN 10 and VLAN 20 as the receive control VLANs..

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 1 through 30. Disable the spanning tree feature and enable flush message receiving on it, and configure VLAN 20 as the receive control VLAN.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 20
[DeviceB-GigabitEthernet1/0/2] quit
```

# Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLANs 1 through 30. Disable the spanning tree feature and enable flush message receiving on it, and configure VLAN 10 as the receive control VLAN.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] smart-link flush enable control-vlan 10
[DeviceB-GigabitEthernet1/0/3] quit
```

4. Configure Device E:

   # Create VLANs 1 through 30.

   ```
   <DeviceE> system-view
   [DeviceE] vlan 1 to 30
   ```

   # Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 1 through 30. Enable flush message receiving on it, and configure VLAN 10 and VLAN 20 as the receive control VLANs.

   ```
   [DeviceE] interface gigabitethernet 1/0/1
   [DeviceE-GigabitEthernet1/0/1] port link-type trunk
   [DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
   [DeviceE-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
   [DeviceE-GigabitEthernet1/0/1] quit
   ```

   # Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 1 through 30. Disable the spanning tree feature and enable flush message receiving on it, and configure VLAN 10 as the receive control VLAN.

   ```
   [DeviceE] interface gigabitethernet 1/0/2
   [DeviceE-GigabitEthernet1/0/2] port link-type trunk
   [DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
   [DeviceE-GigabitEthernet1/0/2] undo stp enable
   [DeviceE-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10
   [DeviceE-GigabitEthernet1/0/2] quit
   ```

   # Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLANs 1 through 30. Disable the spanning tree feature and enable flush message receiving on it, and configure VLAN 20 as the receive control VLAN.

   ```
   [DeviceE] interface gigabitethernet 1/0/3
   [DeviceE-GigabitEthernet1/0/3] port link-type trunk
   [DeviceE-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
   [DeviceE-GigabitEthernet1/0/3] undo stp enable
   [DeviceE-GigabitEthernet1/0/3] smart-link flush enable control-vlan 20
   [DeviceE-GigabitEthernet1/0/3] quit
   ```

5. Configure Device A:

   # Create VLANs 1 through 30.

   ```
   <DeviceA> system-view
   [DeviceA] vlan 1 to 30
   ```

   # Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports, and assign them to VLANs 1 through 30. Enable flush message receiving on them, and configure VLAN 10 and VLAN 20 as the receive control VLANs.

   ```
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] port link-type trunk
   [DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
   [DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
   [DeviceA-GigabitEthernet1/0/1] quit
   ```

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/2] quit
```

6. Verify the configuration:

   You can use the **display smart-link group** command to display the smart link group configuration on a device.

   # Display the smart link group configuration on Device C.

```
[DeviceC] display smart-link group 1
 Smart link group 1 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: NONE
 Preemption delay: 1(s)
 Control VLAN: 10
 Protected VLAN: Reference Instance 1
 Member                      Role    State    Flush-count Last-flush-time
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/1        MASTER  ACTVIE   5           16:37:20 2010/02/21

 GigabitEthernet1/0/2        SLAVE   STANDBY  1           17:45:20 2010/02/21
```

   You can use the **display smart-link flush** command to display the flush messages received on a device.

   # Display the flush messages received on Device B.

```
[DeviceB] display smart-link flush
 Received flush packets                              : 5
 Receiving interface of the last flush packet        : GigabitEthernet1/0/3
 Receiving time of the last flush packet             : 16:25:21 2009/02/21
 Device ID of the last flush packet                  : 000f-e23d-5af0
 Control VLAN of the last flush packet               : 10
```

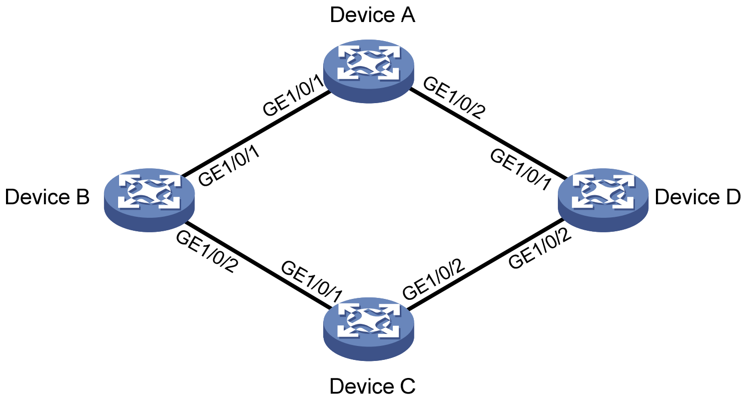
Multiple smart link groups load sharing configuration example

Network requirements

As shown in Figure 24, Device C is a smart link device, and Device A, Device B, and Device D are associated devices. Traffic of VLANs 1 through 200 on Device C are dually uplinked to Device A by Device B and Device D.

Implement dual uplink backup and load sharing on Device C: traffic of VLANs 1 through 100 is uplinked to Device A by Device B; traffic of VLANs 101 through 200 is uplinked to Device A by Device D.

Figure 24 Network diagram



Configuration procedure

1. Configure Device C:

# Create VLAN 1 through VLAN 200. Map VLANs 1 through 100 to MSTI 1. Map VLANs 101 through 200 to MSTI 2, and activate MST region configuration.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 200
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 100
[DeviceC-mst-region] instance 2 vlan 101 to 200
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

# Shut down GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 separately, configure the ports as trunk ports, and assign them to VLAN 1 through VLAN 200.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/2] quit
```

# Create smart link group 1, and configure all VLANs mapped to MSTI 1 as the protected VLANs for smart link group 1.

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

# Configure GigabitEthernet 1/0/1 as the master port and GigabitEthernet 1/0/2 as the slave port for smart link group 1.

```
[DeviceC-smlk-group1] port gigabitethernet1/0/1 master
[DeviceC-smlk-group1] port gigabitethernet1/0/2 slave
```

# Enable role preemption in smart link group 1, enable flush message sending, and configure VLAN 10 as the transmit control VLAN.

```
[DeviceC-smlk-group1] preemption mode role
[DeviceC-smlk-group-1] flush enable control-vlan 10
[DeviceC-smlk-group-1] quit
```

# Create smart link group 2, and configure all VLANs mapped to MSTI 2 as the protected VLANs for smart link group 2.

```
[DeviceC] smart-link group 2
[DeviceC-smlk-group2] protected-vlan reference-instance 2
```

# Configure GigabitEthernet 1/0/1 as the slave port and GigabitEthernet 1/0/2 as the master port for smart link group 2.

```
[DeviceC-smlk-group2] port gigabitethernet1/0/2 master
[DeviceC-smlk-group2] port gigabitethernet1/0/1 slave
```

# Enable role preemption in smart link group 2, enable flush message sending, and configure VLAN 110 as the transmit control VLAN.

```
[DeviceC-smlk-group2] preemption mode role
[DeviceC-smlk-group2] flush enable control-vlan 110
[DeviceC-smlk-group2] quit
```

# Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 again.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

2. Configure Device B:

# Create VLAN 1 through VLAN 200.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 200
```

# Configure GigabitEthernet 1/0/1 as a trunk port and assign it to VLANs 1 through 200. Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceB-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 as a trunk port and assign it to VLANs 1 through 200. Disable the spanning tree feature and enable flush message receiving on it, and configure VLAN 10 and VLAN 110 as the receive control VLANs.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceB-GigabitEthernet1/0/2] quit
```

3. Configure Device D:

# Create VLAN 1 through VLAN 200.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 200
```

# Configure GigabitEthernet 1/0/1 as a trunk port and assign it to VLANs 1 through 200. Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on GigabitEthernet 1/0/1.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceD-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 as a trunk port and assign it to VLANs 1 through 200. Disable the spanning tree feature and enable flush message receiving on it, and configure VLAN 10 and VLAN 110 as the receive control VLANs.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceD-GigabitEthernet1/0/2] quit
```

4. Configure Device A:

# Create VLAN 1 through VLAN 200.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 200
```

# Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports and assign them to VLANs 1 through 200. Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceA-GigabitEthernet1/0/2] quit
```

5. Verify the configuration:

You can use the **display smart-link group** command to display the smart link group configuration on a device.

# Display the smart link group configuration on Device C.

```
[DeviceC] display smart-link group all
 Smart link group 1 information:
 Device ID: 000f-e23d-5af0
 Preemption delay: 1(s)
 Preemption mode: ROLE
 Control VLAN: 10
 Protected VLAN: Reference Instance 1
 Member                     Role    State    Flush-count Last-flush-time
 -----------------------------------------------------------------------------
 GigabitEthernet1/0/1       MASTER  ACTVIE   5           16:37:20 2010/02/21

 GigabitEthernet1/0/2       SLAVE   STANDBY  1           17:45:20 2010/02/21


 Smart link group 2 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 110
 Protected VLAN: Reference Instance 2
 Member                     Role    State    Flush-count Last-flush-time
 -----------------------------------------------------------------------------
 GigabitEthernet1/0/2       MASTER  ACTVIE   5           16:37:20 2010/02/21

 GigabitEthernet1/0/1       SLAVE   STANDBY  1           17:45:20 2010/02/21
```

You can use the **display smart-link flush** command to display the flush messages received on a device.

# Display the flush messages received on Device B.

```
[DeviceB] display smart-link flush
 Received flush packets                             : 5
 Receiving interface of the last flush packet       : GigabitEthernet1/0/2
 Receiving time of the last flush packet            : 16:25:21 2010/02/21
 Device ID of the last flush packet                 : 000f-e23d-5af0
 Control VLAN of the last flush packet              : 10
```

Smart Link and CFD collaboration configuration example

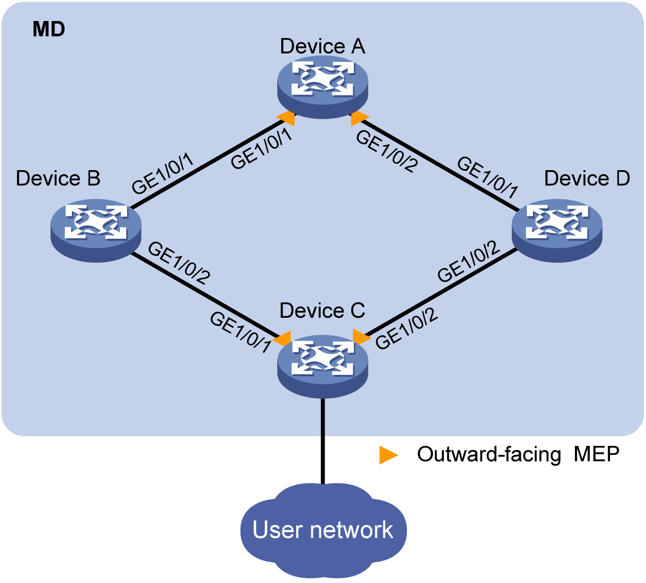
Network requirements

As shown in Figure 25, Device A, Device B, Device C, and Device D form a maintenance domain (MD) of level 5. Device C is a smart link device, and Device A, Device B, and Device D are associated devices. Traffic of VLANs 1 through 200 on Device C is dually uplinked to Device A by Device B and Device D.

Configure the CFD CC function for Smart Link, so that; Traffic of VLANs 1 through 100 is uplinked to Device A by Device C through GigabitEthernet 1/0/1 (master port of smart link group 1). Traffic of VLANs 101 through 200 is uplinked to Device A by Device C through GigabitEthernet 1/0/2 (master port of smart link group 2). When the link between Device C and Device A fails, traffic is rapidly switched to the slave port of each smart link group, and switched back to the master ports after the fault is cleared.

For more information about CFD, see "Configuring CFD."

Figure 25 Network diagram



Configuration procedure

1. Configure Device A:

# Create VLAN 1 through VLAN 200.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 200
```

# Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports and assign them to VLANs 1 through 200. Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceA-GigabitEthernet1/0/2] quit
```

# Enable CFD and create an MD of level 5.

```
[DeviceA] cfd enable
[DeviceA] cfd md MD level 5
```

# Create MA **MA_A** for the MD and configure the MA to serve VLAN 10, and create service instance 1 for the MD and MA.

```
[DeviceA] cfd ma MA_A md MD vlan 10
[DeviceA] cfd service-instance 1 md MD ma MA_A
```

# Create a MEP list in service instance 1, create and enable outward-facing MEP 1002, and enable CCM sending in service instance 1 on GigabitEthernet 1/0/1.

```
[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] interface gigabitethernet 1/0/1
```

```
[DeviceA-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1002 enable
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

# Create MA **MA_B** for the MD and configure the MA to serve VLAN 110, and create service instance 2 for the MD and MA.

```
[DeviceA] cfd ma MA_B md MD vlan 110
[DeviceA] cfd service-instance 2 md MD ma MA_B
```

# Create a MEP list in service instance 2, create and enable outward-facing MEP 1002, and enable CCM sending in service instance 2 on GigabitEthernet 1/0/2.

```
[DeviceA] cfd meplist 2001 2002 service-instance 2
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd mep 2002 service-instance 2 outbound
[DeviceA-GigabitEthernet1/0/2] cfd mep service-instance 2 mep 2002 enable
[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2002 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

2. Configure Device B:

# Create VLAN 1 through VLAN 200.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 200
```

# Configure GigabitEthernet 1/0/1 as a trunk port and assign it to VLANs 1 through 200. Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceB-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 as a trunk port and assign it to VLANs 1 through 200. Disable the spanning tree feature and enable flush message receiving on it, and configure VLAN 10 and VLAN 110 as the receive control VLANs.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceB-GigabitEthernet1/0/2] quit
```

3. Configure Device C:

# Create VLAN 1 through VLAN 200, map VLANs 1 through 100 to MSTI 1, and VLANs 101 through 200 to MSTI 2, and activate MST region configuration.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 200
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 100
[DeviceC-mst-region] instance 2 vlan 101 to 200
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

# Shut down GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable the spanning tree feature on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 separately, configure the ports as trunk ports, and assign them to VLAN 1 through VLAN 200.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/2] quit
```

# Create smart link group 1, and configure all VLANs mapped to MSTI 1 as the protected VLANs for smart link group 1.

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

# Configure GigabitEthernet 1/0/1 as the master port and GigabitEthernet 1/0/2 as the slave port for smart link group 1.

```
[DeviceC-smlk-group1] port gigabitethernet1/0/1 master
[DeviceC-smlk-group1] port gigabitethernet1/0/2 slave
```

# Enable role preemption in smart link group 1, enable flush message sending, and configure VLAN 10 as the transmit control VLAN.

```
[DeviceC-smlk-group1] preemption mode role
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit
```

# Create smart link group 2, and configure all VLANs mapped to MSTI 2 as the protected VLANs for smart link group 2.

```
[DeviceC] smart-link group 2
[DeviceC-smlk-group2] protected-vlan reference-instance 2
```

# Configure GigabitEthernet 1/0/1 as the slave port and GigabitEthernet 1/0/2 as the master port for smart link group 2.

```
[DeviceC-smlk-group2] port gigabitethernet1/0/2 master
[DeviceC-smlk-group2] port gigabitethernet1/0/1 slave
```

# Enable role preemption in smart link group 2, enable flush message sending, and configure VLAN 110 as the transmit control VLAN.

```
[DeviceC-smlk-group2] preemption mode role
[DeviceC-smlk-group2] flush enable control-vlan 110
[DeviceC-smlk-group2] quit
```

# Enable CFD and create an MD of level 5.

```
[DeviceC] cfd enable
[DeviceC] cfd md MD level 5
```

# Create MA **MA_A** for the MD and configure the MA to serve VLAN 10, and create service instance 1 for the MD and MA.

```
[DeviceC] cfd ma MA_A md MD vlan 10
```

```
[DeviceC] cfd service-instance 1 md MD ma MA_A
```

# Create a MEP list in service instance 1, create and enable outward-facing MEP 1001, and enable CCM sending in service instance 1 on GigabitEthernet 1/0/1.

```
[DeviceC] cfd meplist 1001 1002 service-instance 1
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 outbound
[DeviceC-GigabitEthernet1/0/1] cfd mep service-instance 1 mep 1001 enable
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceC-GigabitEthernet1/0/1] quit
```

# Create MA **MA_B** for the MD and configure the MA to serve VLAN 110, and create service instance 2 for the MD and MA.

```
[DeviceC] cfd ma MA_B md MD vlan 110
[DeviceC] cfd service-instance 2 md MD ma MA_B
```

# Create a MEP list in service instance 2, create and enable outward-facing MEP 2001, and enable CCM sending in service instance 2 on GigabitEthernet 1/0/2.

```
[DeviceC] cfd meplist 2001 2002 service-instance 2
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 outbound
[DeviceC-GigabitEthernet1/0/2] cfd mep service-instance 2 mep 2001 enable
[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceC-GigabitEthernet1/0/2] quit
```

# Configure the collaboration between the master port GigabitEthernet 1/0/1 of smart link group 1 and the CC function of CFD, and bring up the port.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port smart-link group 1 track cfd cc
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
```

# Configure the collaboration between the master port GigabitEthernet 1/0/2 of smart link group 2 and the CC function of CFD, and bring up the port.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port smart-link group 2 track cfd cc
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

4. Configure Device D:

# Create VLAN 1 through VLAN 200.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 200
```

# Configure GigabitEthernet 1/0/1 as a trunk port and assign it to VLANs 1 through 200. Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on GigabitEthernet 1/0/1.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceD-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 as a trunk port and assign it to VLANs 1 through 200. Disable the spanning tree feature and enable flush message receiving on it, and configure VLAN 10 and VLAN 110 as the receive control VLANs.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceD-GigabitEthernet1/0/2] quit
```

5. Verify the configuration:

Suppose the optical fiber between Device A and Device B fails. You can use the **display smart-link group** command to display the smart link group configuration on a device.

# Display the smart link group configuration on Device C.

```
[DeviceC] display smart-link group all
 Smart link group 1 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 10
 Protected VLAN: Reference Instance 1
 Member                     Role    State    Flush-count Last-flush-time
 -----------------------------------------------------------------------------
 GigabitEthernet1/0/1       MASTER  DOWN     5           16:37:20 2010/02/21

 GigabitEthernet1/0/2       SLAVE   ACTVIE   3           17:45:20 2010/02/21


 Smart link group 2 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 110
 Protected VLAN: Reference Instance 2
 Member                     Role    State    Flush-count Last-flush-time
 -----------------------------------------------------------------------------
 GigabitEthernet1/0/2       MASTER  ACTVIE   5           16:37:20 2010/02/21

 GigabitEthernet1/0/1       SLAVE   STANDBY  1           17:45:20 2010/02/21
```

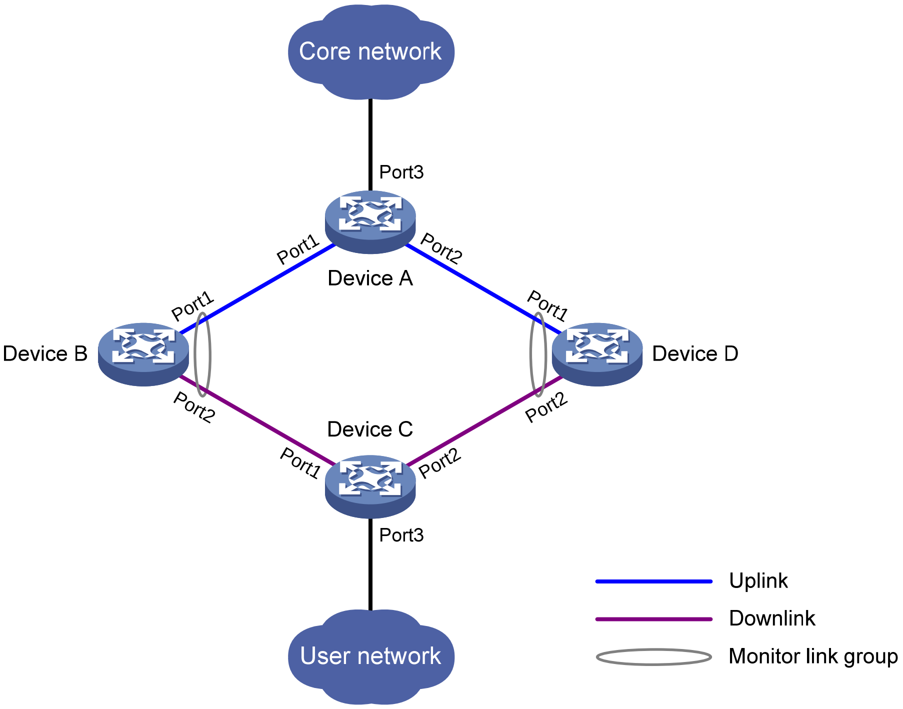
The output shows that master port GigabitEthernet 1/0/1 of smart link group 1 fails, and slave port GigabitEthernet 1/0/2 is in forwarding state.

Configuring Monitor Link

Monitor Link overview

Monitor Link is a port collaboration function. Monitor Link usually works together with Layer 2 topology protocols. The idea is to monitor the states of uplink ports and adapt the up/down state of downlink ports to the up/down state of uplink ports, triggering link switchover on the downstream device in time, as shown in Figure 26.

Figure 26 Monitor Link application scenario



Terminology

Monitor link group

A monitor link group is a set of uplink and downlink ports. A port can belong to only one monitor link group. As shown in Figure 26, ports Port1 and Port2 of Device B and those of Device D each form a monitor link group. Port1 on both devices are uplink ports, and Port2 on both devices are downlink ports.

Uplink/Downlink ports

Uplink port and downlink port are two port roles in monitor link groups:

- Uplink ports are the monitored ports. The state of a monitor link group adapts to that of its member uplink ports. When a monitor link group contains no uplink port or when all the uplink ports are down, the monitor link group becomes down. As long as one member uplink port is up, the monitor link group stays up.

- Downlink ports are the monitoring ports. The state of the downlink ports in a monitor link group adapts to that of the monitor link group. When the state of a monitor link group changes, the state of its member downlink ports change accordingly. The state of the downlink ports in a monitor link group is always consistent with that of the monitor link group.

Uplink/Downlink

The uplink is the link that connects the uplink ports in a monitor link group, and the downlink is the link that connects the downlink ports.

How Monitor Link works

A monitor link group works independently of other monitor link groups. When a monitor link group contains no uplink port or when all its uplink ports are down, the monitor link group goes down and forces all downlink ports down at the same time. When any uplink port goes up, the monitor link group goes up and brings up all the downlink ports.

HP does not recommend manually shutting down or bringing up the downlink ports in a monitor link group.

Configuring Monitor Link

Configuration prerequisites

Make sure that the port is not the member port of any aggregation group or service loopback group.

Creating a monitor link group

Step	Command
1. Enter system view.	**system-view**
2. Create a monitor link group, and enter monitor link group view.	**monitor-link group** *group-id*

Configuring monitor link group member ports

You can configure member ports for a monitor link group either in monitor link group view or interface view. The configurations made in these two views lead to the same result.

You can assign a Layer 2 Ethernet port or Layer 2 aggregate interface to a monitor link group as a member port.

A port can be assigned to only one monitor link group.

Configure uplink ports prior to downlink ports to avoid undesired down/up state changes on the downlink ports.

In monitor link group view

To configure member ports for a monitor link group in monitor link group view:

Step		Command
1.	Enter system view.	**system-view**
2.	Enter monitor link group view.	**monitor-link group** *group-id*
3.	Configure member ports for the monitor link group.	**port** *interface-type interface-number* { **uplink** | **downlink** }

In interface view

To configure member ports for a monitor link group in interface view:

Step		Command
1.	Enter system view.	**system-view**
2.	Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	**interface** *interface-type interface-number*
3.	Configure the current interface as a member of a monitor link group.	**port monitor-link group** *group-id* { **uplink** | **downlink** }

Displaying and maintaining Monitor Link

Task	Command	Remarks
Display monitor link group information.	**display monitor-link group** { *group-id* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Monitor Link configuration example

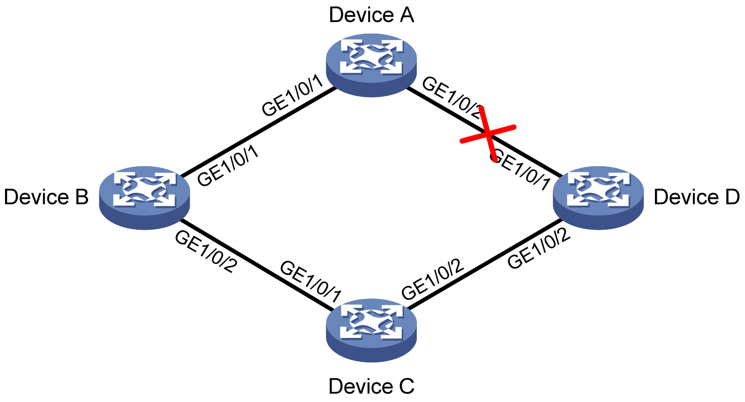
Network requirements

As shown in Figure 27, Device C is a smart link device, and Device A, Device B, and Device D are associated devices. Traffic of VLANs 1 through 30 on Device C is dual-uplinked to Device A through a smart link group.

Implement dual uplink backup on Device C, and make sure that when the link between Device A and Device B (or Device D) fails, Device C can sense the link fault and perform uplink switchover in the smart link group.

For more information about Smart Link, see "Configuring Smart Link."

Figure 27 Network diagram



Configuration procedure

1. Configure Device C:

# Create VLANs 1 through 30, map these VLANs to MSTI 1, and activate MST region configuration.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 30
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

# Disable the spanning tree feature on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 separately, configure them as trunk ports, and assign them to VLANs 1 through 30.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
```

# Create smart link group 1, and configure all the VLANs mapped to MSTI 1 as the protected VLANs for smart link group 1.

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

# Configure GigabitEthernet 1/0/1 as the master port and GigabitEthernet 1/0/2 as the slave port for smart link group 1.

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 master
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 slave
```

# Enable the smart link group to transmit flush messages.

```
[DeviceC-smlk-group1] flush enable
[DeviceC-smlk-group1] quit
```

2. Configure Device A:

   # Create VLANs 1 through 30.

   ```
   <DeviceA> system-view
   [DeviceA] vlan 1 to 30
   ```

   # Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports, assign them to VLANs 1 through 30, and enable flush message receiving on them.

   ```
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] port link-type trunk
   [DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
   [DeviceA-GigabitEthernet1/0/1] smart-link flush enable
   [DeviceA-GigabitEthernet1/0/1] quit
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] port link-type trunk
   [DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
   [DeviceA-GigabitEthernet1/0/2] smart-link flush enable
   [DeviceA-GigabitEthernet1/0/2] quit
   ```

3. Configure Device B:

   # Create VLANs 1 through 30.

   ```
   <DeviceB> system-view
   [DeviceB] vlan 1 to 30
   ```

   # Configure GigabitEthernet 1/0/1 as a trunk port, assign it to VLANs 1 through 30, and enable flush message receiving on it.

   ```
   [DeviceB] interface gigabitethernet 1/0/1
   [DeviceB-GigabitEthernet1/0/1] port link-type trunk
   [DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
   [DeviceB-GigabitEthernet1/0/1] smart-link flush enable
   [DeviceB-GigabitEthernet1/0/1] quit
   ```

   # Configure GigabitEthernet 1/0/2 as a trunk port, assign it to VLANs 1 through 30, disable the spanning tree feature, and enable flush message receiving on it.

   ```
   [DeviceB] interface gigabitethernet 1/0/2
   [DeviceB-GigabitEthernet1/0/2] port link-type trunk
   [DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
   [DeviceB-GigabitEthernet1/0/2] undo stp enable
   [DeviceB-GigabitEthernet1/0/2] smart-link flush enable
   [DeviceB-GigabitEthernet1/0/2] quit
   ```

   # Create monitor link group 1, and then configure GigabitEthernet 1/0/1 as an uplink port and GigabitEthernet 1/0/2 as a downlink port for monitor link group 1.

   ```
   [DeviceB] monitor-link group 1
   [DeviceB-mtlk-group1] port gigabitethernet 1/0/1 uplink
   [DeviceB-mtlk-group1] port gigabitethernet 1/0/2 downlink
   [DeviceB-mtlk-group1] quit
   ```

4. Configure Device D:

   # Create VLANs 1 through 30.

   ```
   <DeviceD> system-view
   [DeviceD] vlan 1 to 30
   ```

# Configure GigabitEthernet 1/0/1 as a trunk port, assign it to VLANs 1 through 30, and enable flush message receiving on it.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable
[DeviceD-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 as a trunk port, assign it to VLANs 1 through 30, disable the spanning tree feature, and enable flush message receiving on it.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable
[DeviceD-GigabitEthernet1/0/2] quit
```

# Create monitor link group 1, and then configure GigabitEthernet 1/0/1 as an uplink port and GigabitEthernet 1/0/2 as a downlink port for monitor link group 1.

```
[DeviceD] monitor-link group 1
[DeviceD-mtlk-group1] port gigabitethernet 1/0/1 uplink
[DeviceD-mtlk-group1] port gigabitethernet 1/0/2 downlink
[DeviceD-mtlk-group1] quit
```

5. Verify the configuration:

   Use the **display monitor-link group** command to display the monitor link group information on devices. For example, when GigabitEthernet 1/0/2 on Device A goes down due to a link fault:

   # Display information about monitor link group 1 on Device B.

```
[DeviceB] display monitor-link group 1
 Monitor link group 1 information:
 Group status: UP
 Last-up-time: 16:37:20 2009/4/21
 Last-down-time: 16:35:26 2009/4/21
 Member                    Role     Status
 ------------------------------------------
 GigabitEthernet1/0/1      UPLINK   UP
 GigabitEthernet1/0/2      DOWNLINK UP
```

   # Display information about monitor link group 1 on Device D.

```
[DeviceD] display monitor-link group 1
 Monitor link group 1 information:
 Group status: DOWN
 Last-up-time: 16:35:27 2009/4/21
 Last-down-time: 16:37:19 2009/4/21
 Member                    Role     Status
 ------------------------------------------
 GigabitEthernet1/0/1      UPLINK   DOWN
 GigabitEthernet1/0/2      DOWNLINK DOWN
```

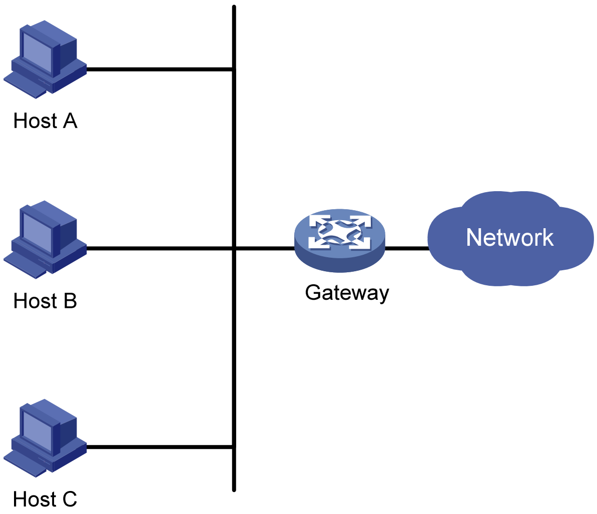
Configuring VRRP (available only on the HP 5500 EI)

- The term *router* in this document refers to both routers and Layer 3 switches.
- You can perform interface-specific VRRP configuration only on Layer 3 Ethernet interfaces, VLAN interfaces, and Layer 3 aggregate interfaces, unless otherwise specified. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).
- VRRP cannot be configured on interfaces in aggregation groups.

VRRP overview

Typically, as shown in Figure 28, you can configure a default route with the gateway as the next hop for every host on a network segment. All packets destined to other network segments are sent over the default route to the gateway, which then forwards the packets. However, when the gateway fails, all the hosts that use the gateway as the default next-hop router fail to communicate with external networks.

Figure 28 LAN networking



Configuring a default route for network hosts facilitates your configuration, but also requires high performance stability of the device that acts as the gateway. Using more egress gateways is a common way to improve system reliability, but introduces the problem of routing among the egresses.

Virtual Router Redundancy Protocol (VRRP) is designed to address this problem. VRRP adds a group of routers that can act as network gateways to a VRRP group, which forms a virtual router. Routers in the VRRP group elect a master through the VRRP election mechanism to act as a gateway, and hosts on a LAN only need to configure the virtual router as their default network gateway.

VRRP is an error-tolerant protocol, which improves the network reliability and simplifies configurations on hosts. On a multicast and broadcast LAN such as Ethernet, VRRP provides highly reliable default links without configuration changes (such as dynamic routing protocols, route discovery protocols) when a router fails, and prevent network interruption because of a single link failure.

VRRP operates in either of the following modes:

- **Standard protocol mode**—Includes two versions VRRPv2 and VRRPv3 based on RFCs. VRRPv2 is based on IPv4, and VRRPv3 is based on IPv6. The two versions implement the same functions but are applied in different network environments. For more information, see "VRRP standard protocol mode."
- **Load balancing mode**—Extends the standard protocol mode and realizes load balancing. For more information, see "VRRP load balancing mode."

VRRP standard protocol mode

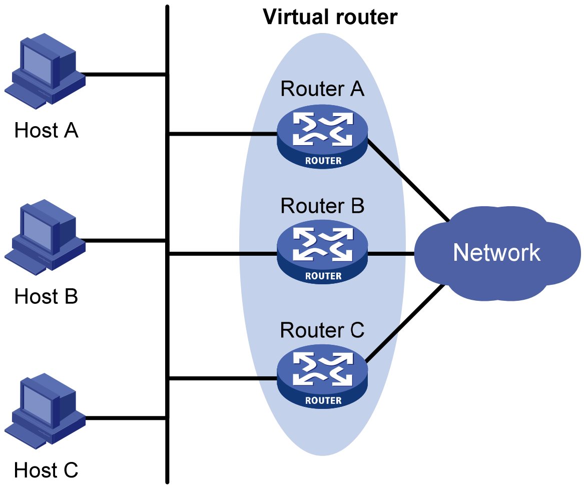
Introduction to VRRP group

VRRP combines a group of routers (including a master and multiple backups) on a LAN into a virtual router called VRRP group.

A VRRP group has the following features:

- A virtual router has a virtual IP address. A host on the LAN only needs to know the IP address of the virtual router and uses the IP address as the next hop of the default route.
- Every host on the LAN communicates with external networks through the virtual router.
- Routers in the VRRP group elect a master that acts as the gateway according to their priorities. The other routers function as the backups. When the master fails, to make sure that the hosts in the network segment can uninterruptedly communicate with the external networks, the backups in the VRRP group elect a new gateway to undertake the responsibility of the failed master.

Figure 29 Network diagram



As shown in Figure 29, Router A, Router B, and Router C form a virtual router, which has its own IP address. Hosts on the Ethernet use the virtual router as the default gateway.

The router with the highest priority among the three routers is elected as the master to act as the gateway, and the other two are backups.

The IP address of the virtual router can be either an unused IP address on the segment where the VRRP group resides or the IP address of an interface on a router in the VRRP group. In the latter case, the router is called the IP address owner.

Only one IP address owner can be configured for a VRRP group.

A router in a VRRP group can be in master, backup, or initialize status.

VRRP priority

VRRP determines the role (master or backup) of each router in a VRRP group by priority. A router with a higher priority is more likely to become the master.

VRRP priority is in the range of 0 to 255. The greater the number, the higher the priority. Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses and priority 255 for the IP address owner. When a router acts as the IP address owner, its running priority is always 255. That is, the IP address owner in a VRRP group acts as the master as long as it operates properly.

Operation mode

A router in a VRRP group operates in either of the following modes:

- **Non-preemptive mode**—When a router in the VRRP group becomes the master, it stays as the master as long as it operates properly, even if a backup is assigned a higher priority later.
- **Preemptive mode**—When a backup finds its priority higher than that of the master, the backup sends VRRP advertisements to start a new master election in the VRRP group and becomes the master. Accordingly, the original master becomes a backup.

Authentication mode

To avoid attacks from unauthorized users, VRRP adds authentication keys into packets for authentication. VRRP provides the following authentication modes:

- **simple**—Simple text authentication

  A router sending a packet fills an authentication key into the packet, and the router receiving the packet compares its local authentication key with that of the received packet. If the two authentication keys are the same, the received VRRP packet is considered legitimate. Otherwise, the received packet is considered invalid.
- **md5**—MD5 authentication

  A router computes the digest of a packet to be sent by using the authentication key and MD5 algorithm and saves the result in the authentication header. The router that receives the packet performs the same operation by using the authentication key and MD5 algorithm, and compares the result with the content in the authentication header. If the results are the same, the router that receives the packet considers the packet an authentic and valid VRRP packet. Otherwise, the router considers the packet invalid.

  On a secure network, you can choose not to set the authentication mode.

VRRP timers

VRRP timers include VRRP advertisement interval timer and VRRP preemption delay timer.

VRRP advertisement interval timer

The master in a VRRP group periodically sends VRRP advertisements to inform the other routers in the VRRP group that it operates properly.

You can adjust the interval for sending VRRP advertisements by setting the VRRP advertisement interval timer. If a backup receives no advertisements in a period three times the interval, the backup regards itself as the master and sends VRRP advertisements to start a new master election.

VRRP preemption delay timer

To avoid frequent state changes among members in a VRRP group and provide the backups enough time to collect information (such as routing information), each backup waits for a period of time (the preemption delay time) after it receives an advertisement with the priority lower than the local priority, then sends VRRP advertisements to start a new master election in the VRRP group and becomes the master.

Packet format

The master multicasts VRRP packets periodically to declare its existence. VRRP packets are also used for checking the parameters of the virtual router and electing the master.

VRRP packets are encapsulated in IP packets, with the protocol number being 112. Figure 30 shows the format of a VRRPv2 packet and Figure 31 shows the format of a VRRPv3 packet.

Figure 30 Format of a VRRPv2 packet

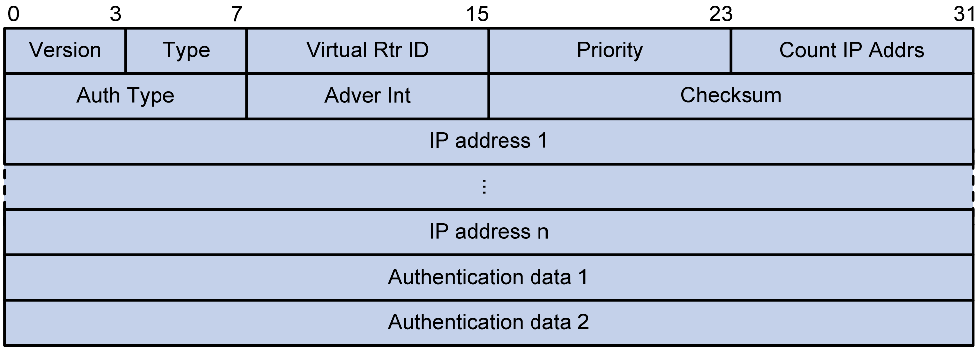
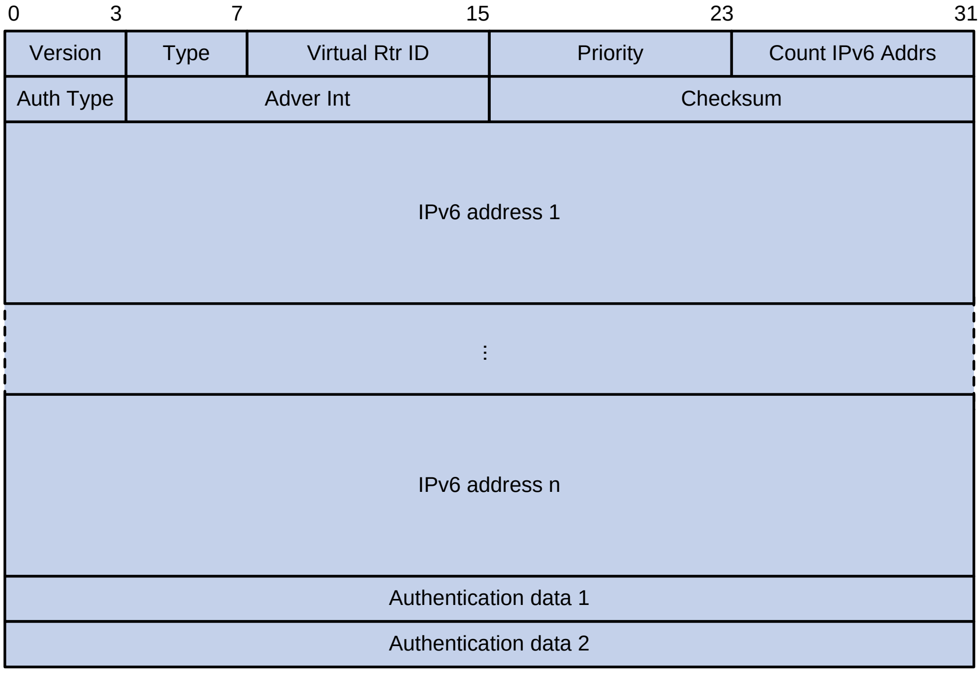


Figure 31 Format of a VRRPv3 packet



A VRRP packet comprises the following fields:

- **Version**—Version number of the protocol, 2 for VRRPv2 and 3 for VRRPv3.
- **Type**—Type of the VRRPv2 or VRRPv3 packet. Only one VRRP packet type is present, that is, VRRP advertisement, which is represented by 1.
- **Virtual Rtr ID (VRID)**—ID of the virtual router, that is, ID of the VRRP group. It ranges from 1 to 255.
- **Priority**—Priority of the router in the VRRP group, in the range of 0 to 255. A greater value represents a higher priority.
- **Count IP Addrs/Count IPv6 Addrs**—Number of virtual IPv4 or IPv6 addresses for the VRRP group. A VRRP group can have multiple virtual IPv4 or IPv6 addresses.
- **Auth Type**—Authentication type. 0 means no authentication, 1 means simple text authentication, and 2 means MD5 authentication. VRRPv3 does not support MD5 authentication.
- **Adver Int**—Interval for sending advertisement packets. For VRRPv2, the interval is in seconds and defaults to 1. For VRRPv3, the interval is in centiseconds and defaults to 100.
- **Checksum**— 16-bit checksum for validating the data in VRRP packets.
- **IP Address/IPv6 Address**—Virtual IPv4 or IPv6 address entry of the VRRP group. The Count IP Addrs or Count IPv6 Addrs field defines the number of the virtual IPv4 or IPv6 addresses.
- **Authentication Data**—Authentication key. This field is used only for simple authentication and is 0 for any other authentication modes.

Principles of VRRP

- Routers in a VRRP group determine their roles by priority. The router with the highest priority is the master, and the others are the backups. The master periodically sends VRRP advertisements to notify the backups that it is operating properly, and each of the backups starts a timer to wait for advertisements from the master.
- In preemptive mode, when a backup receives a VRRP advertisement, it compares the priority in the packet with its own priority. If the priority of the backup is higher, the backup becomes the master. Otherwise, it remains as a backup. With the preemptive mode, a VRRP group always has a router with the highest priority as the master for packet forwarding.
- In non-preemptive mode, a router in the VRRP group remains as a master or backup as long as the master does not fail. A backup does not become the master even if it is configured with a higher priority. The non-preemptive mode helps avoid frequent switchover between the master and backups.
- If the timer of a backup expires but the backup still does not receive any VRRP advertisement, it considers that the master fails. In this case, the backup considers itself as the master and sends VRRP advertisements to start a new master election.

The VRRP group configuration might be different on routers, and network problems might exist, so multiple master routers might exist in one VRRP group. These master routers will elect one master according to their priorities and IP addresses. The router with the highest priority wins the election. If a tie exists in the priority, the router with the highest IP address wins.

After a backup router receives an advertisement, it compares its priority against that carried in the advertisement. If its priority is higher than that carried in the advertisement, it takes over the master.

VRRP tracking

To enable the VRRP tracking function, configure the routers in the VRRP group to operate in preemptive mode first, so that only the router with the highest priority can always operate as the master for packet forwarding.

Tracking a specified interface

The interface tracking function expands the backup functionality of VRRP. It provides backup not only when the interface to which a VRRP group is assigned fails but also when other interfaces (such as uplink interfaces) on the router become unavailable.

If the uplink interface of a router in a VRRP group fails, usually the VRRP group cannot be aware of the uplink interface failure. If the router is the master of the VRRP group, hosts on the LAN are not able to access external networks because of the uplink failure. This problem can be solved by tracking a specified uplink interface. If the tracked uplink interface is down or removed, the priority of the master is automatically decreased by a specified value and a higher priority router in the VRRP group becomes the master.

Monitoring a track entry

By monitoring a track entry, you can:

- Monitor an uplink and change the priority of the router according to the state of the uplink. If the uplink fails, hosts in the LAN cannot access external networks through the router. In this case, the state of the monitored track entry is negative and the priority of the router decreases by a specified value. Then, a higher priority router in the VRRP group becomes the master to maintain the proper communication between the hosts in the LAN and external networks.
- Monitor the master on a backup. When the master fails, the backup immediately preempts as the master to maintain normal communication.

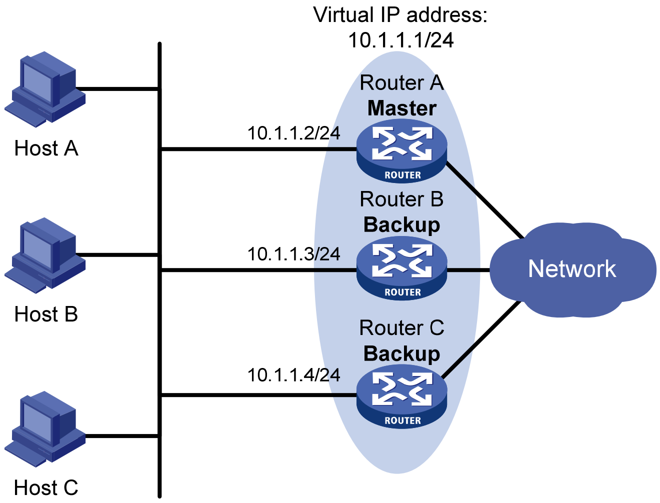
For more information about track entries, see "Configuring track."

VRRP application (taking IPv4-based VRRP for example)

Master/backup

In master/backup mode, only the master forwards packets. When the master fails, a new master is elected from the backups. This mode requires only one VRRP group, in which each router holds a different priority and the one with the highest priority becomes the master, as shown in Figure 32.

Figure 32 VRRP in master/backup mode



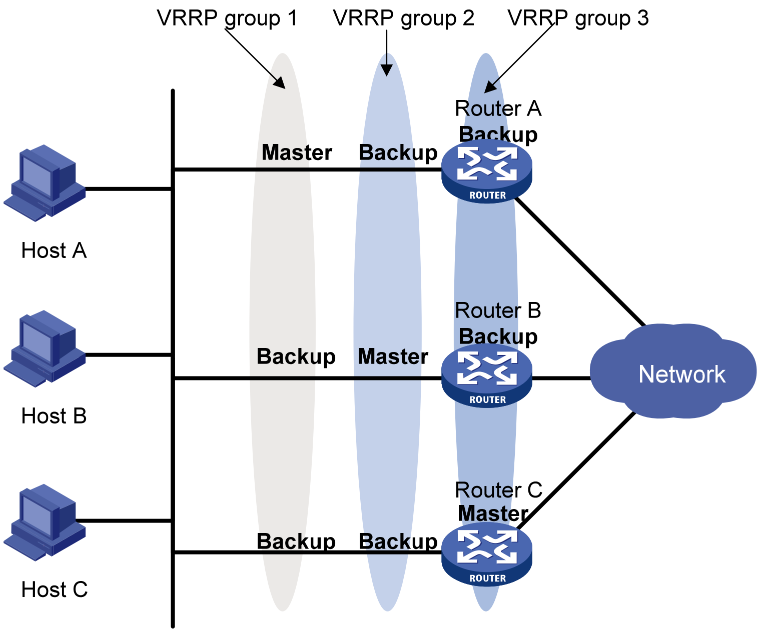
Assume that Router A is the master and therefore can forward packets to external networks, whereas Router B and Router C are backups and are thus in the state of listening. If Router A fails, Router B and Router C elect for a new master to forward packets to hosts on the LAN.

Load sharing

More than one VRRP group can be created on an interface of a router to allow the router to be the master of one VRRP group but a backup of another at the same time.

In load sharing mode, multiple routers provide services simultaneously. This mode requires two or more VRRP groups, each of which comprises a master and one or more backups. The masters of the VRRP groups are assumed by different routers, as shown in Figure 33.

Figure 33 VRRP in load sharing mode



A router can be in multiple VRRP groups and hold a different priority in a different group.

As shown in Figure 33, the following VRRP groups are present:

- **VRRP group 1**—Router A is the master; Router B and Router C are the backups.
- **VRRP group 2**—Router B is the master; Router A and Router C are the backups.
- **VRRP group 3**—Router C is the master; Router A and Router B are the backups.

For load sharing among Router A, Router B, and Router C, hosts on the LAN need to be configured to use VRRP group 1, 2, and 3 as the default gateways. When you configure VRRP priorities, make sure that each router holds such a priority in each VRRP group that it will take the expected role in the group.

VRRP load balancing mode

Overview

When VRRP is operating in standard protocol mode, only the master can forward packets and the backups are in the state of listening. You can create multiple VRRP groups to share the load among multiple routers, but hosts on the LAN need to be configured with different gateways, thus making the configuration complicated.

In load balancing mode, VRRP provides load balancing in addition to virtual gateway redundancy by mapping a virtual IP address to multiple virtual MAC addresses to assign each router in a VRRP group one virtual MAC address. In this way, each router in this VRRP group can respond to ARP requests (in an IPv4 network) or ND requests (in an IPv6 network) from corresponding hosts, so that different hosts can send packets to different routers, and each router in the VRRP group can forward packets. In load balancing mode, you need to create only one VRRP group to balance load among multiple routers, instead of allowing one router to bear the load but other routers to stay idle.

VRRP load balancing mode is based on VRRP standard protocol mode, so mechanisms, such as master election, preemption, and tracking functions, in the standard protocol mode are also supported in the load balancing mode. In addition, VRRP load balancing mode has new mechanisms, which are introduced in the following sections.

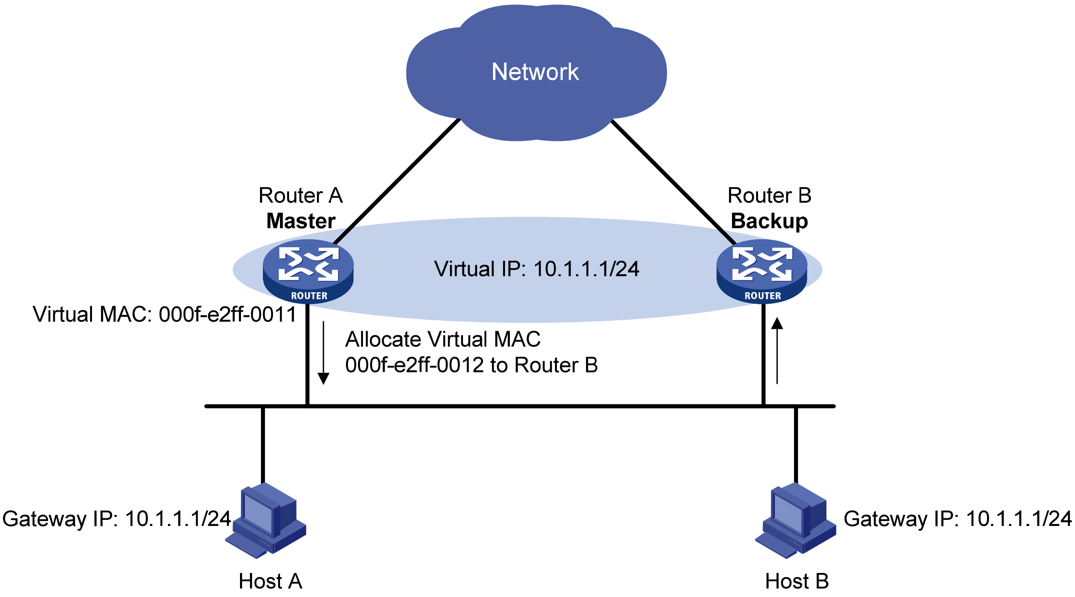
Assigning virtual MAC addresses

When VRRP is operating in load balancing mode, the master assigns virtual MAC addresses to the routers in the VRRP group and answers the ARP requests or ND requests from different hosts. The backup routers, however, do not answer the ARP requests or ND requests from the hosts.

Assume that a VRRP group is operating in an IPv4 network. The following describes how the load balancing mode works:

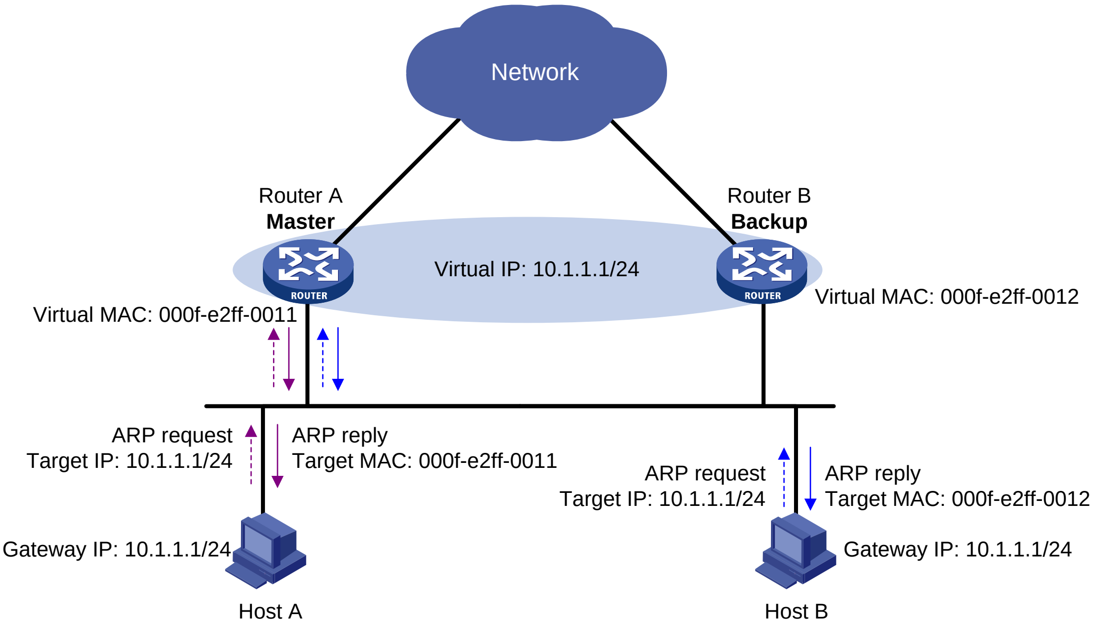
1. The master assigns virtual MAC addresses to the routers (including the master itself and the backups) in the VRRP group. For example, as shown in Figure 34, the virtual IP address of the VRRP group is 10.1.1.1/24; Router A is the master; Router B and Router C are the backups. Router A assigns 000f-e2ff-0011 to itself, and 000f-e2ff-0012 to Router B.

Figure 34 Allocating virtual MAC addresses



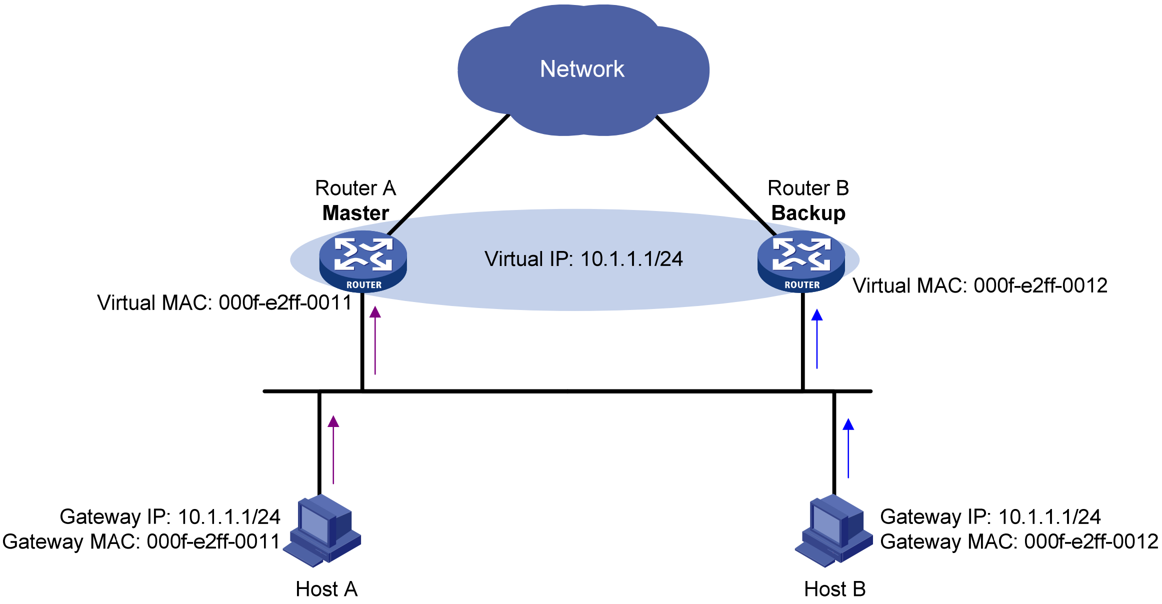
2. After receiving an ARP request destined for the virtual IP address of the VRRP group from a host, the master, based on the load balancing algorithm, uses a corresponding virtual MAC address to answer the ARP request. For example, as shown Figure 35, when Host A sends an ARP request to retrieve the MAC address of gateway 10.1.1.1, the master (Router A), after receiving the request, returns the virtual MAC address of Router A to Host A; when Host B sends an ARP request to retrieve the MAC address of gateway 10.1.1.1, the master (Router A), after receiving the request, returns the virtual MAC address of Router B to Host B.

Figure 35 Answering ARP requests



3. Different hosts send packets to different routers according to the requested virtual MAC addresses. For example, as shown in Figure 36, Host A regards the virtual MAC address of Router A as the gateway MAC address, so it sends packets to Router A for forwarding; Host B regards the virtual MAC address of Router B as the gateway MAC address, so it sends packets to Router B for forwarding.

Figure 36 Sending packets to different routers for forwarding



Virtual forwarder

Creating a virtual forwarder

Virtual MAC addresses help different hosts transmit packets to different routers in a VRRP group. To enable the routers in the VRRP group to forward the packets, be sure to create virtual forwarders (VFs) on the routers. Each VF associates with a virtual MAC address in the VRRP group and forwards packets destined to this virtual MAC address.

The following describes how VFs are created on the routers in a VRRP group:

1. The master assigns virtual MAC addresses to all routers in the VRRP group. After learning its virtual MAC address, a router in the VRRP group creates a VF that corresponds to this MAC address, and becomes the owner of this VF.
2. The router advertises the VF information to the other routers in the VRRP group.
3. After receiving the VF advertisement, each of the other routers creates the advertised VF.

As described in the preceding steps, each router in the VRRP group creates not only a VF corresponding to its virtual MAC address, but also VFs advertised by the other routes in the VRRP group..

VF weight and priority

The weight of a VF indicates the forwarding capability of a router. A higher weight indicates a higher forwarding capability. When the weight is lower than the lower limit of failure, the router cannot be capable of forwarding packets for the hosts.

The priority of a VF determines the VF state. Among the VFs that correspond to the same virtual MAC address on different routers in the VRRP group, the VF with the highest priority is in the active state and is known as the active virtual forwarder (AVF), which forwards packets; other VFs are in the listening state and are known as the listening virtual forwarders (LVFs), which monitor the state of the AVF. The priority value of a VF ranges from 0 to 255, where 255 is reserved for the VF owner. If the weight of a VF owner is higher than or equal to the lower limit of failure, the priority value of the VF owner is 255.

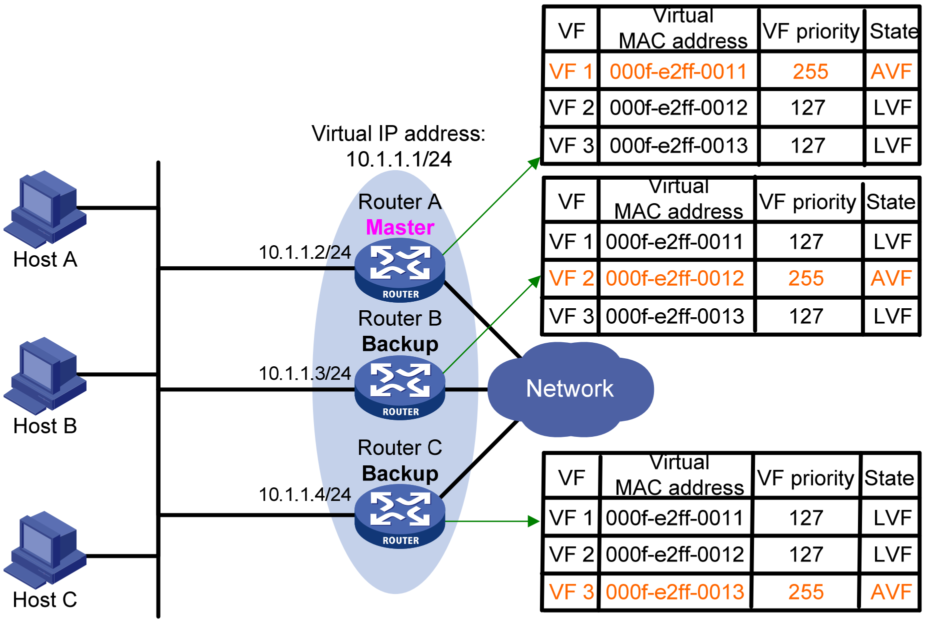
The priority value of a VF is calculated based on its weight:

- If the weight of a VF is higher than or equal to the lower limit of failure, and the router where the VF resides is the owner of the VF, the priority value of the VF is 255.
- If the weight of a VF is higher than or equal to the lower limit of failure, but the router where the VF resides is not the owner of the VF, the priority value of the VF is weight/(number of local AVFs +1)
- If the weight of a VF is lower than the lower limit of failure, the priority value of the VF is 0.

VF backup

The VFs corresponding to a virtual MAC address on different routers in the VRRP group back up one another.

Figure 37 VF information



VF	Virtual MAC address	VF priority	State
VF 1	000f-e2ff-0011	255	AVF
VF 2	000f-e2ff-0012	127	LVF
VF 3	000f-e2ff-0013	127	LVF

VF	Virtual MAC address	VF priority	State
VF 1	000f-e2ff-0011	127	LVF
VF 2	000f-e2ff-0012	255	AVF
VF 3	000f-e2ff-0013	127	LVF

VF	Virtual MAC address	VF priority	State
VF 1	000f-e2ff-0011	127	LVF
VF 2	000f-e2ff-0012	127	LVF
VF 3	000f-e2ff-0013	255	AVF

Figure 37 illustrates the VF information on each router in the VRRP group and how the routers back up one another. The master, Router A, assigns virtual MAC addresses 000f-e2ff-0011, 000f-e2ff-0012, and 000f-e2ff-0013 to itself, Router B, and Router C, respectively. The VFs corresponding to these three virtual MAC addresses, VF 1, VF 2, and VF 3, are created on each of the three routers, and the VFs corresponding to the same virtual MAC address on different routers back up one another. For example, VF 1 on Router A, Router B, and Router C can implement backup.

- Router A is the owner of VF 1, and the priority value of VF 1 on Router A is 255. In this case, VF 1 on Router A acts as the AVF to forward the packets destined for virtual MAC address 000f-e2ff-0011.
- The priority value of VF 1 on Router B and Router C is weight/(number of local AVFs + 1), that is, 255/(1 + 1) =127, which is lower than that of VF 1 on Router A. In this case, VF 1 on both Router B and Router C acts as the LVF to listen to the status of VF 1 on Router A.
- When VF 1 on Router A fails, VF 1 on Router B and Router C elects the one with a higher priority value as the new AVF, responsible for forwarding the packets destined for virtual MAC address 000f-e2ff-0011.

NOTE:

A VF always operates in preemptive mode. When an LVF finds its priority value higher than that in the advertisement sent by the AVF, the LVF declares itself as the AVF.

VF timers

When the AVF on a router fails, the newly elected AVF on another router creates a redirect timer and a timeout timer for the failed AVF.

- **Redirect Timer**—Before this timer times out, the master still uses the virtual MAC address corresponding to the failed AVF to respond to ARP/ND requests from the hosts, and the VF owner can share traffic load if the VF owner resumes normal operation within this time. When this timer times out, the master stops using the virtual MAC address corresponding to the failed AVF to respond to ARP/ND requests from the hosts.

- **Timeout Timer**—The duration that the new AVF takes over the VF owner. Before this timer times out, all the routers in the VRRP group keep the failed AVF, and the new AVF forwards the packets destined for the virtual MAC address corresponding to the failed AVF. When this timer times out, all the routers in the VRRP group remove the failed AVF, and the new AVF stops forwarding the packets destined for the virtual MAC address corresponding to the failed AVF.

VF tracking

The AVF forwards packets destined to the MAC address of the AVF. If the uplink of the AVF fails and no LVF is notified to take over the AVF's work, hosts (on the LAN) that use the MAC address of the AVF as their gateway MAC address cannot access the external network.

This problem can be solved by the VF tracking function. You can monitor the uplink state by using network quality analyzer (NQA) and bidirectional forwarding detection (BFD), and establish the collaboration between the VF and the NQA or between the VF and the BFD through the tracking function. When the uplink fails, the state of the monitored track entry changes to negative and the weight of the VF decreases by a specified value. Then, the VF with a higher priority becomes the AVF and forwards packets.

The VF tracking function can also work on an LVF to monitor its corresponding AVF on another router. When the AVF fails, the LVF immediately takes over the AVF to ensure uninterrupted network communications.

Packet types

VRRP standard protocol mode defines only VRRP advertisement. Only the master in a VRRP group periodically sends VRRP advertisements, and the backups do not send VRRP advertisements.

VRRP load balancing mode defines the following types of packets:

- **Advertisement**—VRRP advertises VRRP group state and information about the VF that is in the active state. Both the master and the backups periodically send VRRP advertisements.
- **Request**—If a backup is not the VF owner, it sends a request to ask the master to assign a virtual MAC address.
- **Reply**—When receiving a request, the master sends a reply to the backup router to assign a virtual MAC address. After receiving the reply, the backup router creates a VF that corresponds to the virtual MAC address, and then becomes the owner of this VF.
- **Release**—When a VF owner fails, the router that takes over its responsibility sends a release after a specified period of time to notify the other routers in the VRRP group to delete the VF of the failed VF owner.

NOTE:

The format of these packets is similar to that of the advertisement in VRRP standard protocol mode except that a packet used in load balancing mode is appended with option field, which contains information for load balancing.

Configuring VRRP for IPv4

VRRP for IPv4 configuration task list

To form a VRRP group, perform the following configurations on each device in the VRRP group.

Complete these tasks to configure VRRP for IPv4:

Task	Remarks
Configuring a VRRP operation mode	Optional.
Specifying the type of MAC addresses mapped to virtual IP addresses	Optional. When VRRP is operating in load balancing mode, this configuration is not effective.
Creating a VRRP group and configuring virtual IP address	Required.
Configuring router priority, preemptive mode and tracking function	Optional.
Configuring VF tracking	Optional. The VF tracking function is effective only when VRRP is operating in load balancing mode.
Configuring VRRP packet attributes	Optional.
Enabling the trap function for VRRP	Optional.

Configuring a VRRP operation mode

VRRP can operate in either of the following modes:

- **Standard protocol mode**—When VRRP is operating in this mode, only the master in a VRRP group is responsible for forwarding packets.
- **Load balancing mode**—When VRRP is operating in this mode, all the routers (master and backups) that have the AVF in a VRRP group can forward packets, thus implementing load balancing.

After the VRRP operation mode is specified on a router, all VRRP groups on the router operate in the specified operation mode.

To configure a VRRP operation mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a VRRP operation mode.	Configure VRRP to operate in standard protocol mode: **undo vrrp mode** Configure VRRP to operate in load balancing mode: **vrrp mode load-balance**	Use either command. By default, VRRP operates in standard protocol mode.

Specifying the type of MAC addresses mapped to virtual IP addresses

After you specify the type of MAC addresses mapped to the virtual IP addresses of VRRP groups and create a VRRP group, the master in the VRRP group uses the specified type of MAC address as the source MAC address for sending packets and uses the specified type of MAC address to answer ARP requests from hosts so that the hosts in the internal network can learn the mapping between the IP address and the MAC address.

The following types of MAC addresses are available to be mapped to the virtual IP address of a VRRP group:

- **Virtual MAC to virtual IP mapping**—By default, a virtual MAC address is automatically created for a VRRP group when the VRRP group is created, and the virtual IP address of the VRRP group is mapped to the virtual MAC address. When such a mapping is adopted, the hosts in the internal network do not need to update the mapping between the IP address and MAC address when the master changes.
- **Real MAC to virtual IP mapping**—In case that an IP address owner exists in a VRRP group, if the virtual IP address is mapped to the virtual MAC address, two MAC addresses are mapped to one IP address. To avoid such as problem, map the virtual IP address of the VRRP group to the real MAC address of an interface to forward the packets from a host to the IP address owner.

Configuration guidelines

- When VRRP is operating in load balancing mode, a virtual IP address is always mapped to a virtual MAC address regardless of which type of MAC addresses are specified to be mapped to virtual IP addresses.
- Specify the type of the MAC addresses mapped to the virtual IP addresses before creating a VRRP group. Otherwise, you cannot change the type of the MAC addresses mapped to virtual IP addresses.
- If VRRP groups with the same ID are created on multiple interfaces of a device, and the VRRP advertisements of these VRRP groups are to be sent through QinQ networks, HP recommends you to map the real MAC addresses of the interfaces to the virtual IP addresses of these VRRP groups. Otherwise, the VRRP advertisements of these VRRP groups cannot be sent successfully.

Configuration procedure

To specify the type of MAC addresses mapped to virtual IP addresses:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify the type of MAC addresses mapped to virtual IP addresses.	**vrrp method** { **real-mac** | **virtual-mac** }	Optional. Virtual MAC address by default.

Creating a VRRP group and configuring virtual IP address

When creating a VRRP group on an interface, configure a virtual IP address for the VRRP group. If the interface connects to multiple sub-networks, you can configure multiple virtual IP addresses for the VRRP group to realize router backup on different sub-networks.

A VRRP group is automatically created when you specify the first virtual IP address for the VRRP group. If you specify another virtual IP address for the VRRP group later, the virtual IP address is added to the virtual IP address list of the VRRP group.

Do not create VRRP groups on the VLAN interface of a super VLAN. Otherwise, network performance might be affected.

Configuration guidelines

- When VRRP is operating in standard protocol mode, the virtual IP address of a VRRP group can be either an unused IP address on the segment where the VRRP group resides or the IP address of an interface on a router in the VRRP group. In the latter case, the router is called the IP address owner.
- When a router is the IP address owner in a VRRP group, HP recommends you not to use the IP address of the interface (virtual IP address of the VRRP group) to establish a neighbor relationship with the adjacent router, that is, not to use the **network** command to enable OSPF on the interface. For more information about **network** command, see *Layer 3—IP Routing Command Reference.*
- When VRRP is operating in load balancing mode, the virtual IP address of a VRRP group cannot be the same as the IP address of any interface in the VRRP group. In other words, in load balancing mode, the VRRP group does not have an IP address owner.
- A VRRP group is removed after you remove all the virtual IP addresses configured for it. In addition, configurations on that VRRP group do not take effect any longer.
- Removal of the VRRP group on the IP address owner causes IP address collision. To solve the collision, modify the IP address of the interface on the IP address owner first and then remove the VRRP group from the interface.
- The virtual IP address of a VRRP group cannot be 0.0.0.0, 255.255.255.255, loopback addresses, non class A/B/C addresses or other illegal IP addresses such as 0.0.0.1.
- A VRRP group operates properly only when the configured virtual IP address and the interface IP address belong to the same segment and are legal host addresses. If the configured virtual IP address and the interface IP address do not belong to the same network segment, or the configured IP address is the network address or network broadcast address of the network segment to which the interface IP address belongs, the state of the VRRP group is always **initialize** though you can perform the configuration successfully. In this case, VRRP does not take effect.

Configuration prerequisites

Before creating a VRRP group and configuring a virtual IP address on an interface, configure an IP address for the interface and make sure that it is in the same network segment as the virtual IP address to be configured.

Configuration procedure

To create a VRRP group and configure a virtual IP address:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter the specified interface view.	**interface** *interface-type interface-number*	N/A
3. Create a VRRP group and configure a virtual IP address for the VRRP group.	**vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*	VRRP group is not created by default.

Configuring router priority, preemptive mode and tracking function

Configuration guidelines

- The running priority of an IP address owner is always 255 and you do not need to configure it. An IP address owner always operates in preemptive mode.
- If you configure an interface to be tracked or a track entry to be monitored on a router that is the IP address owner in a VRRP group, the configuration does not take effect. If the router is not the IP address owner in the VRRP group later, the configuration takes effect.
- If the state of a tracked interface changes from down or removed to up, the priority of the router where the interface resides is automatically restored.
- If the state of a track entry changes from negative or invalid to positive, the priority of the router where the track entry is configured is automatically restored.

Configuration prerequisites

Before you configure router priority, preemptive mode and tracking function, create a VRRP group on an interface and configure a virtual IP address for it.

Configuration procedure

By configuring router priority, preemptive mode, interface tracking, or a track entry, you can determine which router in the VRRP group serves as the master.

To configure router priority, preemptive mode and the tracking function:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter interface view.	**interface** *interface-type interface-number*	N/A
3.	Configure router priority in the VRRP group.	**vrrp vrid** *virtual-router-id* **priority** *priority-value*	Optional. 100 by default.
4.	Configure the router in the VRRP group to operate in preemptive mode and configure preemption delay.	**vrrp vrid** *virtual-router-id* **preempt-mode** [**timer delay** *delay-value*]	Optional. The router in the VRRP group operates in preemptive mode and the preemption delay is 0 seconds by default.
5.	Configure the interface to be tracked.	**vrrp vrid** *virtual-router-id* **track interface** *interface-type interface-number* [**reduced** *priority-reduced*]	Optional. No interface is being tracked by default.
6.	Configure VRRP to track a specified track entry.	**vrrp vrid** *virtual-router-id* **track** *track-entry-number* [**reduced** *priority-reduced* | **switchover**]	Optional. Not configured by default.

Configuring VF tracking

Configuration guidelines

- You can configure the VF tracking function when VRRP is operating in either standard protocol mode or load balancing mode. However, the VF tracking function is effective only when VRRP is operating in load balancing mode.
- By default, the weight of a VF is 255, and its lower limit of failure is 10.
- If the weight of a VF owner is higher than or equal to the lower limit of failure, the priority of the VF owner is always 255 and does not change with the weight value. Therefore, in case of an uplink failure, another VF takes over the VF owner's work and becomes the AVF only when the weight of the VF owner decreases by a properly specified value and becomes lower than the lower limit of failure. In other words, the weight of the VF owner decreases by more than 245.

Configuration prerequisites

Before you configure the VF tracking function, create a VRRP group and configure a virtual IP address for it.

Configuration procedure

VRRP operates in load balancing mode. Assume that you have configured the VF tracking function to monitor the track entry and specified the value by which the weight decreases. When the status of the track entry becomes negative, the weight values of all VFs on the router decrease by the specified value. When the status of the track entry becomes positive or invalid, the weight values of all VFs on the router restore their original values.

If you configure the VF tracking function on an LVF to monitor its corresponding AVF on a specified router, the LVF can take over the AVF immediately when the status of the track entry becomes negative, to ensure uninterrupted network communications.

To configure VF tracking:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter the specified interface view.	**interface** *interface-type interface-number*	N/A
3. Configure VF tracking.	Configure the VF tracking function to monitor a specified track entry and specify the value by which the weight decreases: **vrrp vrid** *virtual-router-id* **weight track** *track-entry-number* [**reduced** *weight-reduced*] Configure the VF tracking function to monitor an AVF on a specified router: **vrrp vrid** *virtual-router-id* **track** *track-entry-number* **forwarder-switchover member-ip** *ip-address*	Use either approach. The VF tracking function is not configured by default.

Configuring VRRP packet attributes

Configuration guidelines

- You might configure different authentication modes and authentication keys for the VRRP groups on an interface. However, the members of the same VRRP group must use the same authentication mode and authentication key.
- Excessive traffic might cause a backup to trigger a change of its status because the backup does not receive any VRRP advertisements for a specified period of time. To solve this problem, prolong the time interval to send VRRP advertisements.
- Configuring different intervals for sending VRRP advertisements on the routers in a VRRP group might cause a backup to trigger a change of its status because the backup does not receive any VRRP advertisements for a specified period of time. To solve this problem, configure the same interval for sending VRRP advertisements on each router in the VRRP group.

Configuration prerequisites

Before you configure the relevant attributes of VRRP packets, create a VRRP group and configure a virtual IP address for it.

Configuration procedure

To configure VRRP packet attributes:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the Differentiated Services Code Point (DSCP) value for VRRP packets.	**vrrp dscp** *dscp-value*	Optional. 48 by default.
3. Enter the specified interface view.	**interface** *interface-type interface-number*	N/A
4. Configure the authentication mode and authentication key when the VRRP groups send and receive VRRP packets.	**vrrp vrid** *virtual-router-id* **authentication-mode** { **md5** | **simple** } [**cipher**] *key*	Optional. Authentication is not performed by default.
5. Configure the time interval for the master in the VRRP group to send VRRP advertisements.	**vrrp vrid** *virtual-router-id* **timer advertise** *adver-interval*	Optional. 1 second by default.
6. Disable TTL check on VRRP packets.	**vrrp un-check ttl**	Optional. Enabled by default. You do not need to create a VRRP group before executing this command.

Enabling the trap function for VRRP

When the trap function is enabled for VRRP, VRRP generates traps with severity level **errors** to report its key events. The traps are sent to the information center of the device, where you can configure whether to output the trap information and the output destination. For how to configure the information center, see *Network Management and Monitoring Configuration Guide*.

To enable the trap function for VRRP:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable the trap function for VRRP.	**snmp-agent trap enable vrrp** [**authfailure** | **newmaster**]	Optional. Enabled by default.

For more information about the **snmp-agent trap enable vrrp** command, see the **snmp-agent trap enable** command in *Network Management and Monitoring Command Reference*.

Displaying and maintaining VRRP for IPv4

Task	Command	Remarks
Display VRRP group status.	**display vrrp** [**verbose**] [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display VRRP group statistics.	**display vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear VRRP group statistics.	**reset vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]	Available in user view

Configuring VRRP for IPv6

VRRP for IPv6 configuration task list

Task	Remarks
Configuring a VRRP operation mode	Optional.
Specifying the type of MAC addresses mapped to virtual IPv6 addresses	Optional. When VRRP is operating in load balancing mode, this configuration is not effective.
Creating a VRRP group and configuring a virtual IPv6 address	Required.
Configuring router priority, preemptive mode and tracking function	Optional.
Configuring VF tracking	Optional. The VF tracking function is effective only when VRRP is operating in load balancing mode.
Configuring VRRP packet attributes	Optional.

Specifying the type of MAC addresses mapped to virtual IPv6 addresses

After you specify the type of MAC addresses mapped to the virtual IPv6 address of VRRP groups and create a VRRP group, the master in the VRRP group uses the specified type of MAC address as the source MAC address for sending packets and uses the specified type of MAC address to answer ND requests from hosts so that the hosts in the internal network can learn the mapping between the IPv6 address and the MAC address.

The following types of MAC addresses are available to be mapped to the virtual IPv6 address of a VRRP group:

- **Virtual MAC to virtual IP mapping**—By default, a virtual MAC address is automatically created for a VRRP group when the VRRP group is created, and the virtual IPv6 address of the VRRP group is mapped to the virtual MAC address. When such a mapping is adopted, the hosts in the internal network do not need to update the mapping between the IPv6 address and the MAC address when the master changes.
- **Real MAC to virtual IP mapping**—In case that an IP address owner exists in a VRRP group, if the virtual IPv6 address is mapped to the virtual MAC address, two MAC addresses are mapped to one IPv6 address. To avoid such as problem, map the virtual IPv6 address of the VRRP group to the real MAC address of an interface to forward the packets from a host to the IP address owner.

When VRRP is operating in load balancing mode, a virtual IPv6 address is always mapped to a virtual MAC address regardless of which type of MAC addresses are specified to be mapped to virtual IPv6 addresses.

Specify the type of the MAC addresses mapped to the virtual IPv6 addresses before creating a VRRP group. Otherwise, you cannot change the type of the MAC addresses mapped to virtual IPv6 addresses.

To specify the type of MAC addresses mapped to virtual IPv6 addresses:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify the type of MAC addresses mapped to virtual IPv6 addresses.	**vrrp ipv6 method** { **real-mac** | **virtual-mac** }	Optional. Virtual MAC address by default.

Creating a VRRP group and configuring a virtual IPv6 address

When creating a VRRP group, configure a virtual IPv6 address for the VRRP group. You can configure multiple virtual IPv6 addresses for a VRRP group.

A VRRP group is automatically created when you specify the first virtual IPv6 address for the VRRP group. If you specify another virtual IPv6 address for the VRRP group later, the virtual IPv6 address is added to the virtual IPv6 address list of the VRRP group.

Do not create VRRP groups on the VLAN interface of a super VLAN. Otherwise, network performance might be affected.

Configuration guidelines

- When a router is the IP address owner in a VRRP group, HP recommends you not to use the IPv6 address of the interface (virtual IPv6 address of the VRRP group) to establish an OSPFv3 neighbor relationship with the adjacent router, that is, not to use the **ospfv3 area** command to enable OSPFv3 on the interface. For more information about **ospfv3 area** command, see *Layer 3—IP Routing Command Reference.*
- When VRRP is operating in load balancing mode, the virtual IPv6 address of a VRRP group cannot be the same as the IPv6 address of any interface in the VRRP group. In other words, a VRRP group does not have an IP address owner in load balancing mode.
- A VRRP group is removed after you remove all the virtual IPv6 addresses in it. In addition, configurations on that VRRP group do not take effect any longer.
- Removal of the VRRP group on the IP address owner causes IP address collision. To resolve the collision, change the IPv6 address of the interface on the IP address owner first and then remove the VRRP group from the interface.

Configuration prerequisites

Before creating a VRRP group and configuring a virtual IPv6 address on an interface, configure an IPv6 address for the interface and make sure that it is in the same network segment as the virtual IPv6 address to be configured.

Configuration procedure

To create a VRRP group and configure its virtual IPv6 address:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter the specified interface view.	**interface** *interface-type interface-number*	N/A
3. Create a VRRP group and configure its virtual IPv6 address, which is a link local address.	**vrrp ipv6 vrid** *virtual-router-id* **virtual-ip** *virtual-address* **link-local**	No VRRP group is created by default. The first virtual IPv6 address of the VRRP group must be a link local address. Only one link local address is allowed in a VRRP group, and must be removed the last.
4. Configure the VRRP group with a virtual IPv6 address, which is a global unicast address.	**vrrp ipv6 vrid** *virtual-router-id* **virtual-ip** *virtual-address*	Optional. By default, no global unicast address is configured as the virtual IPv6 address of a VRRP group.

Configuring router priority, preemptive mode and tracking function

Configuration guidelines

- The running priority of an IP address owner is always 255 and you do not need to configure it. An IP address owner always operates in preemptive mode.

- Interface tracking is not configurable on an IP address owner.
- If you configure an interface to be tracked or a track entry to be monitored on a router that is the IP address owner in a VRRP group, the configuration does not take effect. If the router is not the IP address owner in the VRRP group later, the configuration takes effect.
- If the state of a tracked interface changes from down or removed to up, the priority of the router that owns the interface is automatically restored.
- If the state of a track entry changes from negative or invalid to positive, the priority of the router where the track entry is configured is automatically restored.

Configuration prerequisites

Before you configure router priority, preemptive mode and tracking function, create a VRRP group and configure its virtual IPv6 address.

Configuration procedure

By configuring router priority, preemptive mode, interface tracking, or a track entry, determine which router in the VRRP group serves as the master.

To configure router priority, preemptive mode and interface tracking:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter the specified interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the priority of the router in the VRRP group.	**vrrp ipv6 vrid** *virtual-router-id* **priority** *priority-value*	Optional. 100 by default.
4. Configure the router in the VRRP group to operate in preemptive mode and configure preemption delay of the VRRP group.	**vrrp ipv6 vrid** *virtual-router-id* **preempt-mode** [**timer delay** *delay-value*]	Optional. The router in the VRRP group operates in preemptive mode and the preemption delay is zero seconds by default.
5. Configure the interface to be tracked.	**vrrp ipv6 vrid** *virtual-router-id* **track interface** *interface-type interface-number* [**reduced** *priority-reduced*]	Optional. No interface is being tracked by default.
6. Configure VRRP to track a specified track entry.	**vrrp ipv6 vrid** *virtual-router-id* **track** *track-entry-number* [**reduced** *priority-reduced* | **switchover**]	Optional. Not configured by default.

Configuring VF tracking

Configuration guidelines

- You can configure the VF tracking function when VRRP is operating in either standard protocol mode or load balancing mode. However, the VF tracking function is effective only when VRRP is operating in load balancing mode.
- By default, the weight of a VF is 255, and its lower limit of failure is 10.
- If the weight of a VF owner is higher than or equal to the lower limit of failure, the priority of the VF owner is always 255 and does not change with the weight value. Therefore, if an uplink fails,

another VF takes over the VF owner's work and becomes the AVF only when the weight of the VF owner decreases by a properly specified value and becomes lower than the lower limit of failure. In other words, the weight of the VF owner decreases by more than 245.

Configuration prerequisites

Before you configure the VF tracking function, create a VRRP group and configure a virtual IPv6 address for it.

Configuration procedure

VRRP operates in load balancing mode. Assume that you have configured the VF tracking function to monitor a track entry and specified the value by which the weight decreases. When the status of the track entry becomes negative, the weight values of all VFs on the router decrease by the specified value. When the status of the track entry becomes positive or invalid, the weight values of all VFs on the router restore their original values.

If you configure the VF tracking function on an LVF to monitor its corresponding AVF on a specified router, the LVF can take over the AVF immediately when the status of the track entry becomes negative, to ensure uninterrupted network communications.

To configure VF tracking:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter the specified interface view.	**interface** *interface-type interface-number*	N/A
3.	Configure VF tracking.	Configure the VF tracking function to monitor a specified track entry and specify the value by which the weight decreases: **vrrp ipv6 vrid** *virtual-router-id* **weight track** *track-entry-number* [**reduced** *weight-reduced*] Configure the VF tracking function to monitor an AVF on a specified router: **vrrp ipv6 vrid** *virtual-router-id* **track** *track-entry-number* **forwarder-switchover member-ip** *ipv6-address*	Use either approach. The VF tracking function is not configured by default.

Configuring VRRP packet attributes

Configuration guidelines

- You might configure different authentication modes and authentication keys for the VRRP groups on an interface. However, the members of the same VRRP group must use the same authentication mode and authentication key.
- Excessive traffic might cause a backup to trigger a change of its status because the backup does not receive any VRRP advertisements for a specified period of time. To solve this problem, prolong the time interval to send VRRP advertisements.

- Configuring different intervals for sending VRRP advertisements on the routers in a VRRP group might cause a backup to trigger a change of its status because the backup does not receive any VRRP advertisements for a specified period of time. To solve this problem, configure the same interval for sending VRRP advertisements on each router in the VRRP group.

Configuration prerequisites

Before you configure the relevant attributes of VRRP packets, create a VRRP group and configure a virtual IPv6 address.

Configuration procedure

To configure VRRP packet attributes:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for VRRP packets.	**vrrp ipv6 dscp** *dscp-value*	Optional. 56 by default.
3. Enter the specified interface view.	**interface** *interface-type interface-number*	N/A
4. Configure the authentication mode and authentication key when the VRRP groups send or receive VRRP packets.	**vrrp ipv6 vrid** *virtual-router-id* **authentication-mode simple** [**cipher**] *key*	Optional. Authentication is not performed by default.
5. Configure the time interval for the master in the VRRP group to send VRRP advertisement.	**vrrp ipv6 vrid** *virtual-router-id* **timer advertise** *adver-interval*	Optional. 100 centiseconds by default.

Displaying and maintaining VRRP for IPv6

Task	Command	Remarks
Display VRRP group status.	**display vrrp ipv6** [**verbose**] [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display VRRP group statistics.	**display vrrp ipv6 statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear VRRP group statistics.	**reset vrrp ipv6 statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]	Available in user view

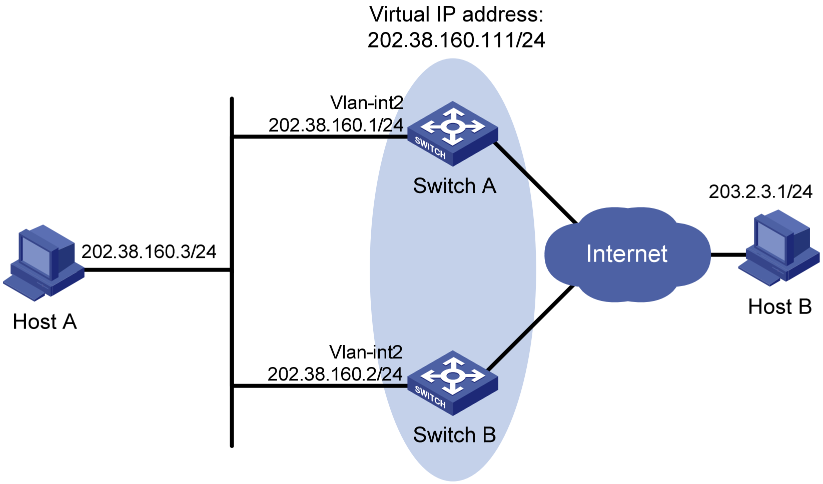
IPv4-based VRRP configuration examples

Single VRRP group configuration example

Network requirements

- Host A wants to access Host B on the Internet, using 202.38.160.111/24 as its default gateway.
- Switch A and Switch B belong to VRRP group 1 with the virtual IP address of 202.38.160.111/24.
- When Switch A operates properly, packets sent from Host A to Host B are forwarded by Switch A; when Switch A fails, packets sent from Host A to Host B are forwarded by Switch B.

Figure 38 Network diagram



Configuration procedure

1. Configure Switch A:

   # Configure VLAN 2.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
```

   # Create VRRP group 1 and set its virtual IP address to 202.38.160.111.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

   # Set the priority of Switch A in VRRP group 1 to 110, which is higher than that of Switch B (100), so that Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

   # Configure Switch A to operate in preemptive mode so that it can become the master whenever it operates properly, and configure the preemption delay as five seconds to avoid frequent status switchover.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

2. Configure Switch B:

   # Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-Vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 202.38.160.2 255.255.255.0
```

# Create VRRP group 1 and set its virtual IP address to 202.38.160.111.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

# Set Switch B to operate in preemptive mode. The preemption delay is five seconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

3. Verify the configuration:

After the configuration, Host B can be pinged successfully on Host A. To verify your configuration, use the **display vrrp verbose** command.

# Display the detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1              Adver Timer  : 1
     Admin Status   : Up             State        : Master
     Config Pri     : 110            Running Pri  : 110
     Preempt Mode   : Yes            Delay Time   : 5
     Auth Type      : None
     Virtual IP     : 202.38.160.111
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 202.38.160.1
```

# Display the detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1              Adver Timer  : 1
     Admin Status   : Up             State        : Backup
     Config Pri     : 100            Running Pri  : 100
     Preempt Mode   : Yes            Delay Time   : 5
     Become Master  : 4200ms left
     Auth Type      : None
     Virtual IP     : 202.38.160.111
     Master IP      : 202.38.160.1
```

The output shows that in VRRP group 1 Switch A is the master, Switch B is the backup and packets sent from Host A to Host B are forwarded by Switch A.

When Switch A fails, you can still ping through Host B on Host A. Use the **display vrrp verbose** command to view the detailed information about the VRRP group on Switch B.

# When Switch A fails, the detailed information about VRRP group 1 on Switch B is displayed.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Master
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
     Auth Type      : None
     Virtual IP     : 202.38.160.111
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 202.38.160.2
```

The output shows that when Switch A fails, Switch B becomes the master, and packets sent from Host A to Host B are forwarded by Switch B.

# After Switch A resumes normal operation, use the **display vrrp verbose** command to display the detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Master
     Config Pri     : 110             Running Pri  : 110
     Preempt Mode   : Yes             Delay Time   : 5
     Auth Type      : None
     Virtual IP     : 202.38.160.111
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 202.38.160.1
```

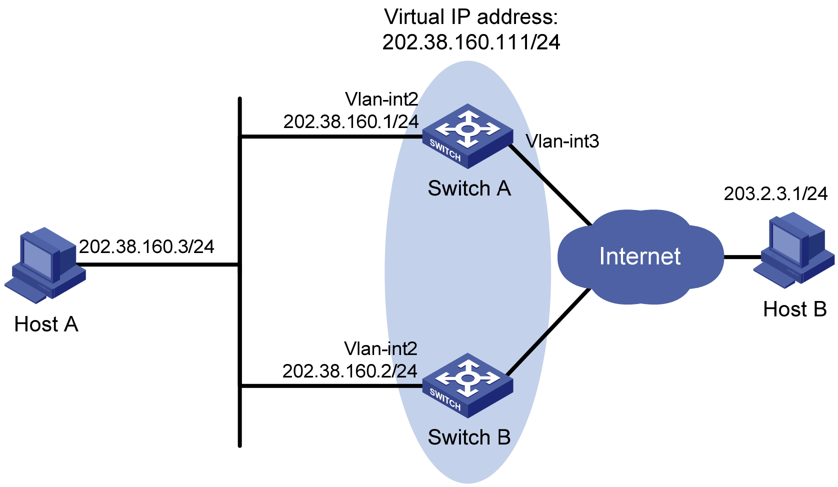
The output shows that after Switch A resumes normal operation, it becomes the master, and packets sent from host A to host B are forwarded by Switch A.

VRRP interface tracking configuration example

Network requirements

- Host A wants to access Host B on the Internet, using 202.38.160.111/24 as its default gateway.
- Switch A and Switch B belong to VRRP group 1 with the virtual IP address of 202.38.160.111/24.
- If Switch A operates properly, packets sent from Host A to Host B are forwarded by Switch A. If VLAN-interface 3 through which Switch A connects to the Internet is not available, packets sent from Host A to Host B are forwarded by Switch B.
- To prevent attacks to the VRRP group from illegal users by using spoofed packets, configure the authentication mode as plain text to authenticate the VRRP packets in VRRP group 1, and specify the authentication key as **hello**.

Figure 39 Network diagram



Configuration procedure

1. Configure Switch A:

   # Configure VLAN 2.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
```

   # Create a VRRP group 1 and set its virtual IP address to 202.38.160.111.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

   # Configure the priority of Switch A in the VRRP group to 110, which is higher than that of Switch B (100), so that Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

   # Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

   # Set the interval for Master to send VRRP advertisement to four seconds.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 timer advertise 4
```

   # Configure Switch A to operate in preemptive mode, so that it can become the master whenever it operates properly. Configure the preemption delay as five seconds to avoid frequent status switchover.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

   # Set VLAN interface 3 on Switch A to be tracked, and configure the amount by which the priority value decreases to be more than 10 (30 in this example), so that when VLAN-interface 3 fails, the priority of Switch A in VRRP group 1 decreases to a value lower than 100 and thus Switch B can become the master.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track interface vlan-interface 3 reduced 30
```

2. Configure Switch B:

   # Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB] vlan 2
```

```
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 202.38.160.2 255.255.255.0
```

# Create a VRRP group 1 and set its virtual IP address to 202.38.160.111.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

# Configure the authentication mode of the VRRP group as **simple** and authentication key as **hello**.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

# Set the interval for master to send VRRP advertisement to four seconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 timer advertise 4
```

# Configure Switch B to operate in preemptive mode, so that Switch B can become the master after the priority of Switch A decreases to a value lower than 100. Configure the preemption delay as five seconds to avoid frequent status switchover.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

3. Verify the configuration:

After the configuration, Host B can be pinged successfully on Host A. To verify your configuration, use the **display vrrp verbose** command.

# Display the detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 4
     Admin Status   : Up              State        : Master
     Config Pri     : 110             Running Pri  : 110
     Preempt Mode   : Yes             Delay Time   : 5
     Auth Type      : Simple          Key          : ******
     Virtual IP     : 202.38.160.111
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 202.38.160.1
   VRRP Track Information:
     Track Interface: Vlan3          State : Up                Pri Reduced : 30
```

# Display the detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 4
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 2200ms left
     Auth Type      : Simple          Key          : ******
     Virtual IP     : 202.38.160.111
     Master IP      : 202.38.160.1
```

The output shows that in VRRP group 1 Switch A is the master, Switch B is the backup and packets sent from Host A to Host B are forwarded by Switch A.

If interface VLAN-interface 3 through which Switch A connects to the Internet is not available, you can still ping Host B successfully on Host A. To view the detailed information about the VRRP group, use the **display vrrp verbose** command.

# If VLAN-interface 3 on Switch A is not available, the detailed information about VRRP group 1 on Switch A is displayed.

```
[SwitchA-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 4
     Admin Status   : Up              State        : Backup
     Config Pri     : 110             Running Pri  : 80
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 2200ms left
     Auth Type      : Simple          Key          : ******
     Virtual IP     : 202.38.160.111
     Master IP      : 202.38.160.2
   VRRP Track Information:
     Track Interface: Vlan3          State : Down              Pri Reduced : 30
```

# When VLAN-interface 3 on Switch A is not available, the detailed information about VRRP group 1 on Switch B is displayed.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 4
     Admin Status   : Up              State        : Master
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
     Auth Type      : Simple          Key          : ******
     Virtual IP     : 202.38.160.111
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 202.38.160.2
```

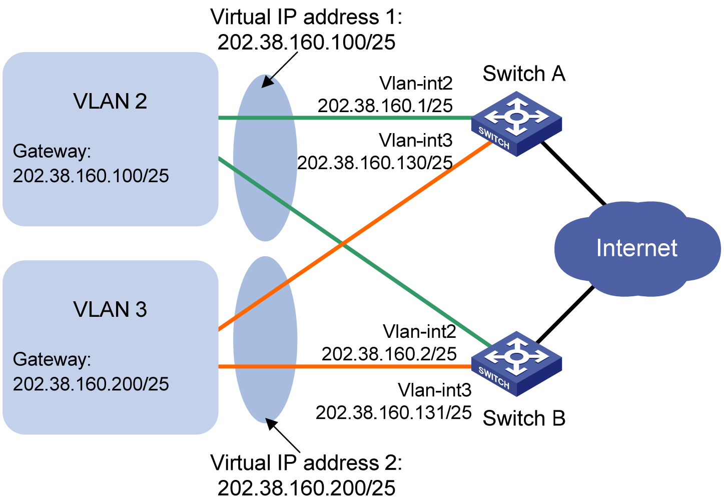
The output shows that when VLAN-interface 3 on Switch A is not available, the priority of Switch A is reduced to 80 and it becomes the backup. Switch B becomes the master and packets sent from Host A to Host B are forwarded by Switch B.

VRRP with multiple VLANs configuration example

Network requirements

- Hosts in VLAN 2 use 202.38.160.100/25 as their default gateway and hosts in VLAN 3 use 202.38.160.200/25 as their default gateway.
- Switch A and Switch B belong to both VRRP group 1 and VRRP group 2. The virtual IP address of VRRP group 1 is 202.38.160.100/25, and that of VRRP group 2 is 202.38.160.200/25.
- In VRRP group 1, Switch A has a higher priority than Switch B. In VRRP group 2, Switch B has a higher priority than Switch A. In this case, hosts in VLAN 2 and VLAN 3 can communicate with external networks through Switch A and Switch B, respectively, and when Switch A or Switch B fails, the hosts can use the other switch to communicate with external networks to avoid communication interruption.

Figure 40 Network diagram



Configuration procedure

1. Configure Switch A:

# Configure VLAN 2.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 202.38.160.1 255.255.255.128
```

# Create a VRRP group 1 and set its virtual IP address to 202.38.160.100.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.100
```

# Configure the priority of Switch A in VRRP group 1 as 110, which is higher than that of Switch B (100), so that Switch A can become the master in VRRP group 1.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
[SwitchA-Vlan-interface2] quit
```

# Configure VLAN 3.

```
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/6
```

```
[SwitchA-vlan3] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 202.38.160.130 255.255.255.128
```

# Create a VRRP group 2 and set its virtual IP address to 202.38.160.200.

```
[SwitchA-Vlan-interface3] vrrp vrid 2 virtual-ip 202.38.160.200
```

2. Configure Switch B:

# Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 202.38.160.2 255.255.255.128
```

# Create a VRRP group 1 and set its virtual IP address to 202.38.160.100.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.100
[SwitchB-Vlan-interface2] quit
```

# Configure VLAN 3.

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/6
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 202.38.160.131 255.255.255.128
```

# Create a VRRP group 2 and set its virtual IP address to 202.38.160.200.

```
[SwitchB-Vlan-interface3] vrrp vrid 2 virtual-ip 202.38.160.200
```

# Configure the priority of Switch B in VRRP group 2 to 110, which is higher than that of Switch A (100), so that Switch B can become the master in VRRP group 2.

```
[SwitchB-Vlan-interface3] vrrp vrid 2 priority 110
```

3. Verify the configuration:

To verify your configuration, use the **display vrrp verbose** command.

# Display the detailed information about the VRRP group on Switch A.

```
[SwitchA-Vlan-interface3] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                Adver Timer  : 1
     Admin Status   : Up               State        : Master
     Config Pri     : 110              Running Pri  : 110
     Preempt Mode   : Yes              Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 202.38.160.100
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 202.38.160.1
   Interface Vlan-interface3
     VRID           : 2                Adver Timer  : 1
     Admin Status   : Up                State        : Backup
     Config Pri     : 100               Running Pri  : 100
     Preempt Mode   : Yes               Delay Time   : 0
     Become Master  : 2200ms left
     Auth Type      : None
     Virtual IP     : 202.38.160.200
     Master IP      : 202.38.160.131
```

# Display the detailed information about the VRRP group on Switch B.

```
[SwitchB-Vlan-interface3] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer  : 1
     Admin Status   : Up                State        : Backup
     Config Pri     : 100               Running Pri  : 100
     Preempt Mode   : Yes               Delay Time   : 0
     Become Master  : 2200ms left
     Auth Type      : None
     Virtual IP     : 202.38.160.100
     Master IP      : 202.38.160.1
   Interface Vlan-interface3
     VRID           : 2                 Adver Timer  : 1
     Admin Status   : Up                State        : Master
     Config Pri     : 110               Running Pri  : 110
     Preempt Mode   : Yes               Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 202.38.160.200
     Virtual MAC    : 0000-5e00-0102
     Master IP      : 202.38.160.131
```

The output shows that in VRRP group 1 Switch A is the master, Switch B is the backup and hosts with the default gateway of 202.38.160.100/25 accesses the Internet through Switch A; in VRRP group 2 Switch A is the backup, Switch B is the master and hosts with the default gateway of 202.38.160.200/25 accesses the Internet through Switch B.

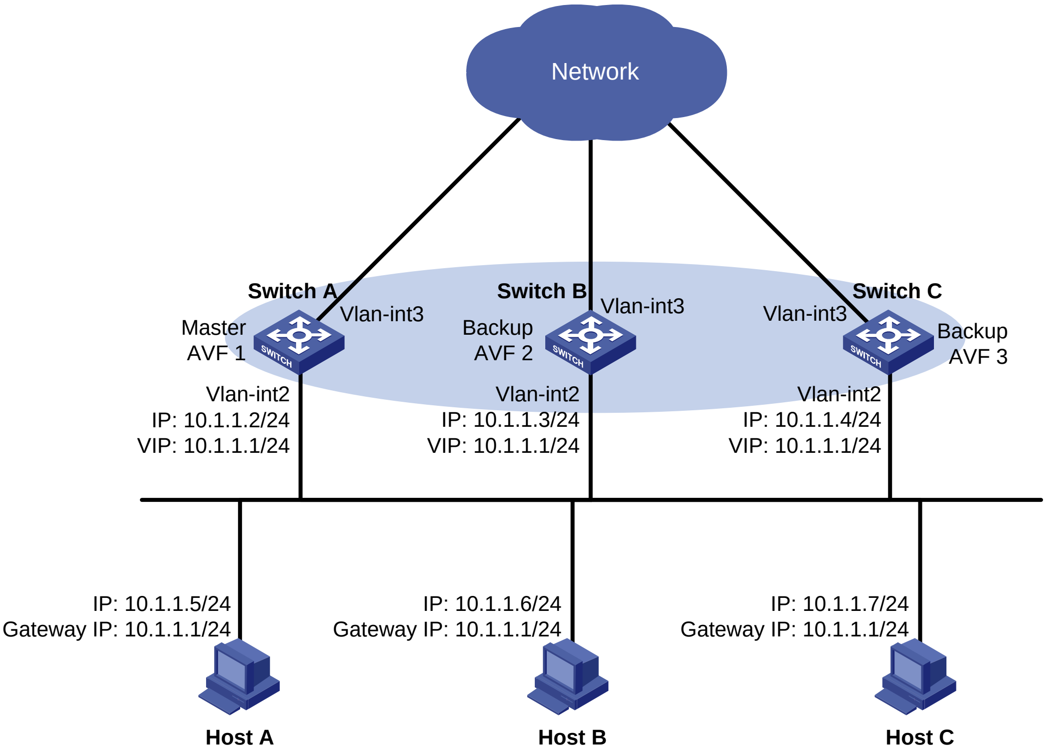
VRRP load balancing mode configuration example

Network requirements

- Switch A, Switch B, and Switch C belong to VRRP group 1 with the virtual IP address of 10.1.1.1/24.
- Hosts on network segment 10.1.1.0/24 use 10.1.1.1/24 as their default gateway. Use the VRRP group to make sure that when a gateway (Switch A, Switch B, or Switch C) fails, the hosts on the LAN can access external networks through another gateway.
- VRRP group 1 is operating in load balancing mode to make good use of network resources.
- Configure a track entry on Switch A, Switch B, and Switch C to monitor their own VLAN-interface 3. When the interface on Switch A, Switch B, or Switch C fails, the weight of the corresponding switch decreases so that another switch with a higher weight can take over.

- Configure track entries on Switch C to monitor Switch A and Switch B. When Switch A or Switch B fails, Switch C immediately takes over the AVF on Switch A or Switch B.

Figure 41 Network diagram



Configuration procedure

1. Configure Switch A:

# Configure VLAN 2.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
```

# Configure VRRP to operate in load balancing mode.

```
[SwitchA] vrrp mode load-balance
```

# Create VRRP group 1 and configure its virtual IP address as 10.1.1.1.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.2 24
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
```

# Set the priority of Switch A in VRRP group 1 to 120, which is higher than that of Switch B (110) and that of Switch C (100), so that Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 120
```

# Configure Switch A to operate in preemptive mode, so that it can become the master whenever it operates properly; configure the preemption delay as five seconds to avoid frequent status switchover.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
[SwitchA-Vlan-interface2]  quit
```

# Create track entry 1 to associate with the physical status of VLAN-interface 3 on Switch A. When the track entry becomes negative, it means that the interface fails.

```
[SwitchA] track 1 interface vlan-interface 3
```

# Configure VF tracking to monitor track entry 1 and specify the value by which the weight decreases, making the weight of Switch A decrease by more than 245 (250 in this example) when track entry 1 turns to negative. In such a case, another router with a higher weight can take over.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp vrid 1 weight track 1 reduced 250
```

2. Configure Switch B:

# Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
```

# Configure VRRP to operate in load balancing mode.

```
[SwitchB] vrrp mode load-balance
```

# Create VRRP group 1 and configure its virtual IP address as 10.1.1.1.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.1.1.3 24
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
```

# Set the priority of Switch B in VRRP group 1 to 110, which is higher than that of Switch C (100), so that Switch B can become the master when Switch A fails.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 priority 110
```

# Set Switch B to operate in preemptive mode. The preemption delay is five seconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
[SwitchB-Vlan-interface2] quit
```

# Create track entry 1 to associate with the physical status of VLAN-interface 3 on Switch B. When the track entry becomes negative, it means that the interface fails.

```
[SwitchB] track 1 interface vlan-interface 3
```

# Configure VF tracking to monitor track entry 1 and specify the value by which the weight decreases, making the weight of Switch B decrease by more than 245 (250 in this example) when track entry 1 turns to negative. In such a case, another router with a higher weight can take over.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 weight track 1 reduced 250
```

3. Configure Switch C:

# Configure VLAN 2.

```
<SwitchC> system-view
[SwitchC] vlan 2
[SwitchC-vlan2] port gigabitethernet 1/0/5
[SwitchC-vlan2] quit
```

# Configure VRRP to operate in load balancing mode.

```
[SwitchC] vrrp mode load-balance
```

# Create VRRP group 1 and configure its virtual IP address as 10.1.1.1.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ip address 10.1.1.4 24
[SwitchC-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
```

# Set Switch C to operate in preemptive mode. The preemption delay is five seconds.

```
[SwitchC-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
[SwitchC-Vlan-interface2] quit
```

# Create track entry 1 to associate with the physical status of VLAN-interface 3 on Switch C. When the track entry becomes negative, it means that the interface fails.

```
[SwitchC] track 1 interface vlan-interface 3
```

# Configure VF tracking to monitor track entry 1 and specify the value by which the weight decreases, making the weight of Switch C decrease by more than 245 (250 in this example) when track entry 1 turns to negative. In such a case, another router with a higher weight can take over.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] vrrp vrid 1 weight track 1 reduced 250
[SwitchC-Vlan-interface2] quit
```

# Create track entries 2 and 3 to monitor Switch A and Switch B, respectively. If a track entry becomes negative, it indicates that the corresponding switch fails.

```
[SwitchC] bfd echo-source-ip 1.2.3.4
[SwitchC] track 2 bfd echo interface vlan-interface 2 remote ip 10.1.1.2 local ip
10.1.1.4
[SwitchC] track 3 bfd echo interface vlan-interface 2 remote ip 10.1.1.3 local ip
10.1.1.4
```

# Configure VF tracking to monitor track entry 2. When track entry 2 becomes negative, the LVF on Switch C whose corresponding AVF is on the switch with the IP address of 10.1.1.2 immediately becomes active. Switch C takes over the AVF on Switch A.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] vrrp vrid 1 track 2 forwarder-switchover member-ip 10.1.1.2
```

# Configure VF tracking to monitor track entry 3. When track entry 2 becomes negative, the LVF on Switch C whose corresponding AVF is on the switch with the IP address of 10.1.1.3 immediately becomes active. Switch C takes over the AVF on Switch B.

```
[SwitchC-Vlan-interface2] vrrp vrid 1 track 3 forwarder-switchover member-ip 10.1.1.3
```

4. Verify the configuration:

After the configuration, Host A can ping the external network. To verify your configuration, use the **display vrrp verbose** command.

# Display the detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Master
     Config Pri     : 120             Running Pri  : 120
     Preempt Mode   : Yes             Delay Time   : 5
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.2 (Local, Master)
                      10.1.1.3 (Backup)
                      10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-0011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 255
     Active         : local
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : 10.1.1.3
    Forwarder 03
     State          : Listening
     Virtual MAC    : 000f-e2ff-0013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 127
     Active         : 10.1.1.4
   Forwarder Weight Track Information:
     Track Object   : 1              State : Positive       Weight Reduced : 250
```

# Display the detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Backup
     Config Pri     : 110             Running Pri  : 110
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 4200ms left
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.3 (Local, Backup)
                      10.1.1.2 (Master)
                      10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Listening
     Virtual MAC    : 000f-e2ff-0011 (Learnt)
     Owner ID       : 0000-5e01-1101
     Priority       : 127
     Active         : 10.1.1.2
    Forwarder 02
     State          : Active
     Virtual MAC    : 000f-e2ff-0012 (Owner)
     Owner ID       : 0000-5e01-1103
     Priority       : 255
     Active         : local
    Forwarder 03
     State          : Listening
     Virtual MAC    : 000f-e2ff-0013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 127
     Active         : 10.1.1.4
   Forwarder Weight Track Information:
     Track Object   : 1              State : Positive       Weight Reduced : 250
```

# Display the detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 4200ms left
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.4 (Local, Backup)
                      10.1.1.2 (Master)
                      10.1.1.3 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Listening
     Virtual MAC    : 000f-e2ff-0011 (Learnt)
     Owner ID       : 0000-5e01-1101
     Priority       : 127
     Active         : 10.1.1.2
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : 10.1.1.3
    Forwarder 03
```

```
     State          : Active
     Virtual MAC    : 000f-e2ff-0013 (Owner)
     Owner ID       : 0000-5e01-1105
     Priority       : 255
     Active         : local
   Forwarder Weight Track Information:
     Track Object   : 1              State : Positive       Weight Reduced : 250
   Forwarder Switchover Track Information:
     Track Object   : 2              State : Positive
       Member IP    : 10.1.1.2
     Track Object   : 3              State : Positive
       Member IP    : 10.1.1.3
```

The output shows that in VRRP group 1, Switch A is the master and Switch B and Switch C are the backups. Each switch has one AVF and two LVFs that act as the backups.

# When VLAN-interface 3 on Switch A fails, use the **display vrrp verbose** command to display the detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Master
     Config Pri     : 120             Running Pri  : 120
     Preempt Mode   : Yes             Delay Time   : 5
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.2 (Local, Master)
                      10.1.1.3 (Backup)
                      10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 0 Active
     Config Weight  : 255
     Running Weight : 5
    Forwarder 01
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 0
     Active         : 10.1.1.4
    Forwarder 02
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 0
     Active         : 10.1.1.3
    Forwarder 03
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 0
     Active         : 10.1.1.4
   Forwarder Weight Track Information:
     Track Object   : 1                State : Negative       Weight Reduced : 250
```

# Use the **display vrrp verbose** command to display the detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer  : 1
     Admin Status   : Up                State        : Backup
     Config Pri     : 100               Running Pri  : 100
     Preempt Mode   : Yes               Delay Time   : 5
     Become Master  : 4200ms left
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.4 (Local, Backup)
                      10.1.1.2 (Master)
                      10.1.1.3 (Backup)
   Forwarder Information: 3 Forwarders 2 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-0011 (Take Over)
     Owner ID       : 0000-5e01-1101
     Priority       : 85
     Active         : local
     Redirect Time  : 93 secs
     Time-out Time  : 1293 secs
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 85
     Active         : 10.1.1.3
    Forwarder 03
     State          : Active
     Virtual MAC    : 000f-e2ff-0013 (Owner)
     Owner ID       : 0000-5e01-1105
     Priority       : 255
     Active         : local
   Forwarder Weight Track Information:
     Track Object   : 1              State : Positive       Weight Reduced : 250
   Forwarder Switchover Track Information:
     Track Object   : 2              State : Positive
       Member IP    : 10.1.1.2
     Track Object   : 3              State : Positive
       Member IP    : 10.1.1.3
```

The output shows that when VLAN interface 3 on Switch A fails, the weight of the AVF on Switch A decreases to 5, which is lower than the lower limit of failure. All VFs on Switch A turn to initialized state and cannot be used for packet forwarding. The VF corresponding to MAC address 000f-e2ff-0011 on Switch C becomes the AVF, and Switch C takes over Switch A for packet forwarding.

# When the timeout timer (about 1800 seconds) expires, display the detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 4200ms left
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.4 (Local, Backup)
                      10.1.1.2 (Master)
                      10.1.1.3 (Backup)
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : 10.1.1.3
    Forwarder 03
     State          : Active
     Virtual MAC    : 000f-e2ff-0013 (Owner)
     Owner ID       : 0000-5e01-1105
     Priority       : 255
     Active         : local
   Forwarder Weight Track Information:
     Track Object   : 1              State : Positive       Weight Reduced : 250
   Forwarder Switchover Track Information:
     Track Object   : 2              State : Positive
```

```
       Member IP    : 10.1.1.2
     Track Object   : 3              State : Positive
       Member IP    : 10.1.1.3
```

The output shows that when the timeout timer expires, the VF corresponding to virtual MAC address 000f-e2ff-0011 is removed, and does not forward the packets destined for the MAC address any more.

# When Switch A fails, use the **display vrrp verbose** command to display the detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Master
     Config Pri     : 110             Running Pri  : 110
     Preempt Mode   : Yes             Delay Time   : 5
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.3 (Local, Master)
                      10.1.1.4 (Backup)
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 02
     State          : Active
     Virtual MAC    : 000f-e2ff-0012 (Owner)
     Owner ID       : 0000-5e01-1103
     Priority       : 255
     Active         : local
    Forwarder 03
     State          : Listening
     Virtual MAC    : 000f-e2ff-0013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 127
     Active         : 10.1.1.4
   Forwarder Weight Track Information:
     Track Object   : 1              State : Positive       Weight Reduced : 250
```

The output shows that when Switch A fails, Switch B becomes the master because its priority is higher than that of Switch C.

# When Switch B fails, use the **display vrrp verbose** command to display the detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
```

```
Interface GigabitEthernet1/0/1
  VRID           : 1                Adver Timer  : 1
  Admin Status   : Up               State        : Master
  Config Pri     : 100              Running Pri  : 100
  Preempt Mode   : Yes              Delay Time   : 5
  Auth Type      : None
  Virtual IP     : 10.1.1.1
  Member IP List : 10.1.1.4 (Local, Master)
Forwarder Information: 2 Forwarders 2 Active
  Config Weight  : 255
  Running Weight : 255
 Forwarder 02
  State          : Active
  Virtual MAC    : 000f-e2ff-0012 (Take Over)
  Owner ID       : 0000-5e01-1103
  Priority       : 85
  Active         : local
  Redirect Time  : 93 secs
  Time-out Time  : 1293 secs
 Forwarder 03
  State          : Active
  Virtual MAC    : 000f-e2ff-0013 (Owner)
  Owner ID       : 0000-5e01-1105
  Priority       : 255
  Active         : local
Forwarder Weight Track Information:
  Track Object   : 1               State : Positive       Weight Reduced : 250
Forwarder Switchover Track Information:
  Track Object   : 2               State : Negative
    Member IP    : 10.1.1.2
  Track Object   : 3               State : Negative
    Member IP    : 10.1.1.3
```

The output shows that when Switch B fails, Switch C becomes the master, and Forwarder 02 on Switch C immediately becomes active. Switch C takes over the AVF on Switch B.

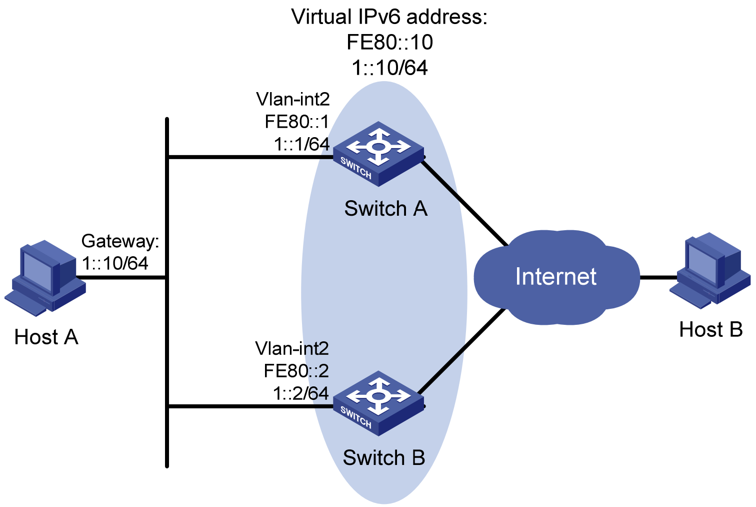
IPv6-based VRRP configuration examples

Single VRRP group configuration example

Network requirements

- Switch A and Switch B belong to VRRP group 1 with the virtual IP addresses of 1::10/64 and FE80::10.
- Host A wants to access Host B on the Internet, and learns 1::10/64 as its default gateway through RA messages sent by the switches.
- When Switch A operates properly, packets sent from Host A to Host B are forwarded by Switch A; when Switch A fails, packets sent from Host A to Host B are forwarded by Switch B.

Figure 42 Network diagram



Configuration procedure

1. Configure Switch A:

   # Configure VLAN 2.

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
[SwitchA-Vlan-interface2] ipv6 address 1::1 64
```

   # Create a VRRP group 1 and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

   # Set the priority of Switch A in VRRP group 1 to 110, which is higher than that of Switch B (100), so that Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

   # Configure Switch A to operate in preemptive mode so that it can become the master whenever it operates properly, and configure the preemption delay as five seconds to avoid frequent status switchover.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

   # Enable Switch A to send RA messages, so that Host A can learn the default gateway address.

```
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
```

2. Configure Switch B:

   # Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB] ipv6
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
```

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
```

# Create a VRRP group 1 and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

# Configure Switch B to operate in preemptive mode, with the preemption delay set to 5 seconds.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

# Enable Switch B to send RA messages, so that Host A can learn the default gateway address.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

3. Verify the configuration:

After the configuration, Host B can be pinged successfully on Host A. To verify your configuration, use the **display vrrp ipv6 verbose** command.

# Display the detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 100
     Admin Status   : Up              State        : Master
     Config Pri     : 110             Running Pri  : 110
     Preempt Mode   : Yes             Delay Time   : 5
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::1
```

# Display the detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 100
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 4200ms left
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Master IP      : FE80::1
```

The output shows that in VRRP group 1 Switch A is the master, Switch B is the backup and packets sent from Host A to Host B are forwarded by Switch A.

When Switch A fails, you can still successfully ping Host B on Host A. To view the detailed information about the VRRP group on Switch B, use the **display vrrp ipv6 verbose** command.

# When Switch A fails, the detailed information about VRRP group 1 on Switch B is displayed.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode        : Standard
     Run Method      : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID            : 1                Adver Timer  : 100
     Admin Status    : Up               State        : Master
     Config Pri      : 100              Running Pri  : 100
     Preempt Mode    : Yes              Delay Time   : 5
     Auth Type       : None
     Virtual IP      : FE80::10
                       1::10
     Virtual MAC     : 0000-5e00-0201
     Master IP       : FE80::2
```

The output shows that when Switch A fails, Switch B becomes the master, and packets sent from Host A to Host B are forwarded by Switch B.

# After Switch A resumes normal operation, use the **display vrrp ipv6 verbose** command to display the detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode        : Standard
     Run Method      : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID            : 1                Adver Timer  : 100
     Admin Status    : Up               State        : Master
     Config Pri      : 110              Running Pri  : 110
     Preempt Mode    : Yes              Delay Time   : 5
     Auth Type       : None
     Virtual IP      : FE80::10
                       1::10
     Virtual MAC     : 0000-5e00-0201
     Master IP       : FE80::1
```

The output shows that after Switch A resumes normal operation, it becomes the master, and packets sent from host A to host B are forwarded by Switch A.

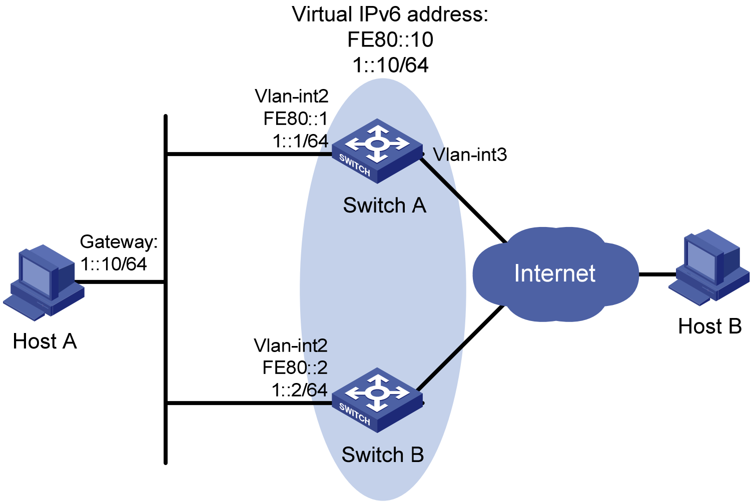
VRRP interface tracking configuration example

Network requirements

- Switch A and Switch B belong to VRRP group 1 with the virtual IP addresses of 1::10/64 and FE80::10.
- Host A wants to access Host B on the Internet, and learns 1::10/64 as its default gateway through RA messages sent by the switches.

- When Switch A operates properly, packets sent from Host A to Host B are forwarded by Switch A. If VLAN-interface 3 through which Switch A connects to the Internet is not available, packets sent from Host A to Host B are forwarded by Switch B.
- To prevent attacks to the VRRP group from illegal users by using spoofed packets, configure the authentication mode as plain text to authenticate the VRRP packets in VRRP group 1, and specify the authentication key as **hello**.

Figure 43 Network diagram



Configuration procedure

1. Configure Switch A:

# Configure VLAN 2.

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
[SwitchA-Vlan-interface2] ipv6 address 1::1 64
```

# Create a VRRP group 1 and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

# Set the priority of Switch A in VRRP group 1 to 110, which is higher than that of Switch B (100), so that Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

# Set the authentication mode for VRRP group 1 to **simple** and authentication key to **hello**.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 authentication-mode simple hello
```

# Set the VRRP advertisement interval to 400 centiseconds.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 timer advertise 400
```

# Configure Switch A to operate in preemptive mode, so that it can become the master whenever it operates properly; configure the preemption delay as five seconds to avoid frequent status switchover.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

# Set VLAN-interface 3 on Switch A to be tracked, and configure the amount by which the priority value decreases to be more than 10 (30 in this example), so that when VLAN interface 3 fails, the priority of Switch A in VRRP group 1 decreases to a value lower than 100 and thus Switch B can become the master.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 track interface vlan-interface 3 reduced
30
```

# Enable Switch A to send RA messages, so that Host A can learn the default gateway address.

```
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
```

2. Configure Switch B:

# Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB] ipv6
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
```

# Create a VRRP group 1 and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

# Set the authentication mode for VRRP group 1 to **simple** and authentication key to **hello**.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 authentication-mode simple hello
```

# Set the VRRP advertisement interval to 400 centiseconds.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 timer advertise 400
```

# Configure Switch B to operate in preemptive mode, so that Switch B can become the master after the priority of Switch A decreases to a value lower than 100. Configure the preemption delay as five seconds to avoid frequent status switchover.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

# Enable Switch B to send RA messages, so that Host A can learn the default gateway address.

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
```

3. Verify the configuration:

After the configuration, Host B can be pinged successfully on Host A. To verify the configuration, use the **display vrrp ipv6 verbose** command.

# Display the detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 400
     Admin Status   : Up              State        : Master
     Config Pri     : 110             Running Pri  : 110
     Preempt Mode   : Yes             Delay Time   : 5
     Auth Type      : Simple          Key          : ******
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::1
   VRRP Track Information:
     Track Interface: Vlan3          State : Up                Pri Reduced : 30
```

# Display the detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 400
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 4200ms left
     Auth Type      : Simple          Key          : ******
     Virtual IP     : FE80::10
                      1::10
     Master IP      : FE80::1
```

The output shows that in VRRP group 1 Switch A is the master, Switch B is the backup and packets sent from Host A to Host B are forwarded by Switch A.

When interface VLAN-interface 3 on Switch A is not available, you can still ping Host B successfully on Host A. To view the detailed information about the VRRP group, use the **display vrrp ipv6 verbose** command.

# When interface VLAN-interface 3 on Switch A is not available, the detailed information about VRRP group 1 on Switch A is displayed.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 400
     Admin Status   : Up              State        : Backup
     Config Pri     : 110             Running Pri  : 80
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 4200ms left
     Auth Type      : Simple          Key          : ******
     Virtual IP     : FE80::10
                      1::10
     Master IP      : FE80::2
   VRRP Track Information:
     Track Interface: Vlan3        State : Down              Pri Reduced : 30
```

# When interface VLAN-interface 3 on Switch A is not available, the detailed information about VRRP group 1 on Switch B is displayed.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer  : 400
     Admin Status   : Up                State        : Master
     Config Pri     : 100               Running Pri  : 100
     Preempt Mode   : Yes               Delay Time   : 5
     Auth Type      : Simple            Key          : ******
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::2
```

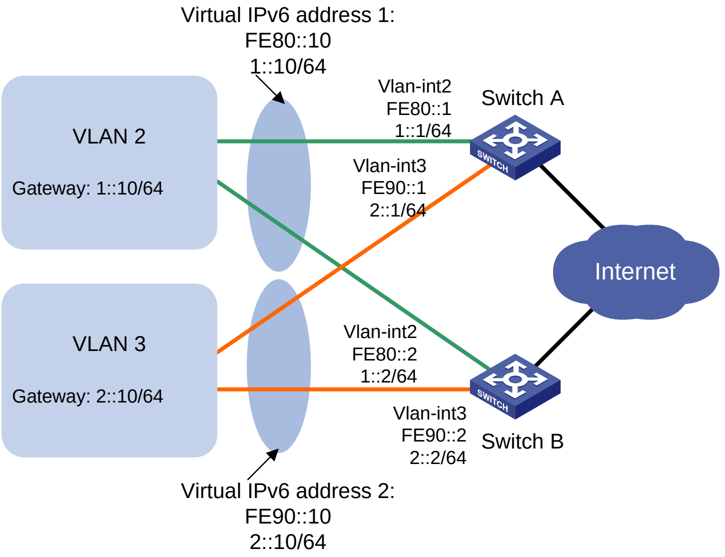
The output shows that when VLAN-interface 3 on Switch A is not available, the priority of Switch A is reduced to 80 and Switch A becomes the backup. Switch B becomes the master and packets sent from Host A to Host B are forwarded by Switch B.

VRRP with multiple VLANs configuration example

Network requirements

- Switch A and Switch B belong to both VRRP group 1 and VRRP group 2. The virtual IPv6 addresses of VRRP group 1 are 1::10/64 and FE80::10, and those of VRRP group 2 are 2::10/64 and FE90::10.
- Hosts in VLAN 2 learn 1::10/64 as their default gateway and hosts in VLAN 3 learn 2::10/64 as their default gateway through RA messages sent by the switches.
- In VRRP group 1, Switch A has a higher priority than Switch B. In VRRP group 2, Switch B has a higher priority than Switch A. In this case, hosts in VLAN 2 and VLAN 3 can communicate with external networks through Switch A and Switch B, respectively, and when Switch A or Switch B fails, the hosts can use the other switch to communicate with external networks to avoid communication interruption.

Figure 44 Network diagram



Configuration procedure

1. Configure Switch A:

# Configure VLAN 2.

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
[SwitchA-Vlan-interface2] ipv6 address 1::1 64
```

# Create VRRP group 1 and set its virtual IPv6 addresses to FE80::10 to 1::10.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

# Set the priority of Switch A in VRRP group 1 to 110, which is higher than that of Switch B (100), so that Switch A can become the master in VRRP group 1.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
[SwitchA-Vlan-interface2] quit
```

# Enable Switch A to send RA messages, so that hosts in VLAN 2 can learn the default gateway address.

```
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
[SwitchA-Vlan-interface2] quit
```

# Configure VLAN 3.

```
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/6
[SwitchA-vlan3] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ipv6 address fe90::1 link-local
[SwitchA-Vlan-interface3] ipv6 address 2::1 64
```

# Create VRRP group 2 and set its virtual IPv6 addresses to FE90::10 and 2::10.

```
[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip 2::10
```

# Enable Switch A to send RA messages, so that hosts in VLAN 3 can learn the default gateway address.

```
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
```

2. Configure Switch B:

   # Configure VLAN 2.

   ```
   <SwitchB> system-view
   [SwitchB] ipv6
   [SwitchB-vlan2] port gigabitethernet 1/0/5
   [SwitchB-vlan2] quit
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
   [SwitchB-Vlan-interface2] ipv6 address 1::2 64
   ```

   # Create VRRP group 1 and set its virtual IPv6 addresses to FE80::10 and 1::10.

   ```
   [SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
   [SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
   [SwitchB-Vlan-interface2] quit
   ```

   # Enable Switch B to send RA messages, so that hosts in VLAN 2 can learn the default gateway address.

   ```
   [SwitchB-Vlan-interface2] undo ipv6 nd ra halt
   [SwitchB-Vlan-interface2] quit
   ```

   # Configure VLAN 3.

   ```
   [SwitchB] vlan 3
   [SwitchB-vlan3] port gigabitethernet 1/0/6
   [SwitchB-vlan3] quit
   [SwitchB] interface vlan-interface 3
   [SwitchB-Vlan-interface3] ipv6 address fe90::2 link-local
   [SwitchB-Vlan-interface3] ipv6 address 2::2 64
   ```

   # Create VRRP group 2 and set its virtual IPv6 addresses to FE90::10 and 2::10.

   ```
   [SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
   [SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip 2::10
   ```

   # Set the priority of Switch B in VRRP group 2 to 110, which is higher than that of Switch A (100), so that Switch B can become the master in VRRP group 2.

   ```
   [SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 priority 110
   ```

   # Enable Switch B to send RA messages, so that hosts in VLAN 3 can learn the default gateway address.

   ```
   [SwitchB-Vlan-interface3] undo ipv6 nd ra halt
   ```

3. Verify the configuration:

   To verify the configuration, use the **display vrrp ipv6 verbose** command.

   # Display the detailed information about the VRRP group on Switch A.

   ```
   [SwitchA-Vlan-interface3] display vrrp ipv6 verbose
    IPv6 Standby Information:
        Run Mode       : Standard
        Run Method     : Virtual MAC
   ```

```
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                Adver Timer  : 100
     Admin Status   : Up               State        : Master
     Config Pri     : 110              Running Pri  : 110
     Preempt Mode   : Yes              Delay Time   : 0
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::1
   Interface Vlan-interface3
     VRID           : 2                Adver Timer  : 100
     Admin Status   : Up               State        : Backup
     Config Pri     : 100              Running Pri  : 100
     Preempt Mode   : Yes              Delay Time   : 0
     Become Master  : 2200ms left
     Auth Type      : None
     Virtual IP     : FE90::10
                      2::10
     Master IP      : FE90::2
```

# Display the detailed information about the VRRP group on Switch B.

```
[SwitchB-Vlan-interface3] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                Adver Timer  : 100
     Admin Status   : Up               State        : Backup
     Config Pri     : 100              Running Pri  : 100
     Preempt Mode   : Yes              Delay Time   : 0
     Become Master  : 2200ms left
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Master IP      : FE80::1
   Interface Vlan-interface3
     VRID           : 2                Adver Timer  : 100
     Admin Status   : Up               State        : Master
     Config Pri     : 110              Running Pri  : 110
     Preempt Mode   : Yes              Delay Time   : 0
     Auth Type      : None
     Virtual IP     : FE90::10
                      2::10
     Virtual MAC    : 0000-5e00-0202
     Master IP      : FE90::2
```

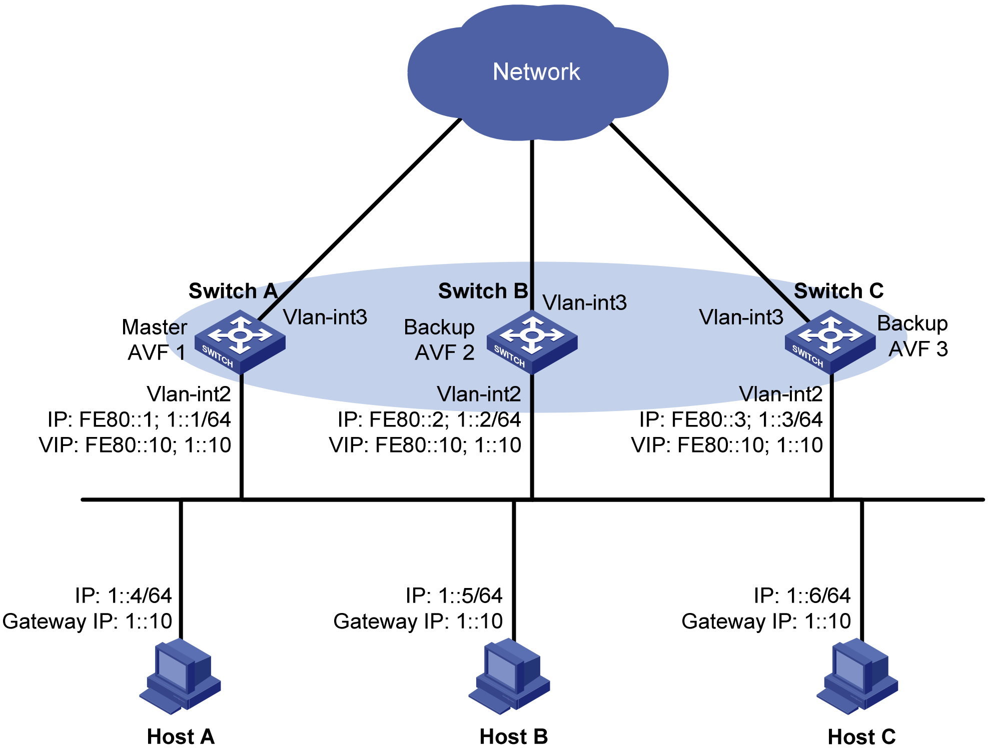
The output shows that in VRRP group 1 Switch A is the master, Switch B is the backup and hosts with the default gateway of 1::10/64 accesses the Internet through Switch A; in VRRP group 2 Switch A is the backup, Switch B is the master and hosts with the default gateway of 2::10/64 accesses the Internet through Switch B.

VRRP load balancing mode configuration example

Network requirements

- Switch A, Switch B, and Switch C belong to VRRP group 1 with the virtual IPv6 addresses of FE80::10 and 1::10.
- Hosts on network segment 1::/64 learn 1::10 as their default gateway through RA messages sent by the switches. Use the VRRP group to make sure that when a gateway (Switch A, Switch B, or Switch C) fails, the hosts on the LAN can access the external network through another gateway.
- VRRP group 1 is operating in load balancing mode to make good use of network resources.
- Configure a track entry on Switch A, Switch B, and Switch C to monitor their own VLAN-interface 3. When the interface on Switch A, Switch B, or Switch C fails, the weight of the corresponding switch decreases so that another switch with a higher weight can take over.

Figure 45 Network diagram



Configuration procedure

1. Configure Switch A:

# Configure VLAN 2.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
```

# Configure VRRP to operate in load balancing mode.

```
[SwitchA] vrrp mode load-balance
```

# Create VRRP group 1 and configure its virtual IPv6 addresses as FE80::10 and 1::10.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
[SwitchA-Vlan-interface2] ipv6 address 1::1 64
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

# Set the priority of Switch A in VRRP group 1 to 120, which is higher than that of Switch B (110) and that of Switch C (100), so that Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 120
```

# Configure Switch A to operate in preemptive mode so that it can become the master whenever it operates properly; configure the preemption delay as five seconds to avoid frequent status switchover.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

# Enable Switch A to send RA messages so that hosts on network segment 1::/64 can learn the default gateway address.

```
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
[SwitchA-Vlan-interface2]  quit
```

# Create track entry 1 to associate with the physical status of VLAN-interface 3 on Switch A. When the track entry becomes negative, it means that the interface fails.

```
[SwitchA] track 1 interface vlan-interface 3
```

# Configure VF tracking to monitor track entry 1 and specify the value by which the weight decreases, making the weight of Switch A decrease by more than 245 (250 in this example) when track entry 1 turns to negative. In such a case, another router with a higher weight can take over.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 weight track 1 reduced 250
```

2. Configure Switch B:

# Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
```

# Configure VRRP to operate in load balancing mode.

```
[SwitchB] vrrp mode load-balance
```

# Create VRRP group 1 and configure its virtual IPv6 addresses as FE80::10 and 1::10.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

# Set the priority of Switch B in VRRP group 1 to 110, which is higher than that of Switch C (100) so that Switch B can become the master when Switch A fails.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

# Set Switch B to operate in preemptive mode and set the preemption delay to five seconds.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

# Enable Switch B to send RA messages so that hosts on network segment 1::/64 can learn the default gateway address.

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
[SwitchB-Vlan-interface2]  quit
```

# Create track entry 1 to associate with the physical status of VLAN-interface 3 on Switch B. When the track entry becomes negative, it means that the interface fails.

```
[SwitchB] track 1 interface vlan-interface 3
```

# Configure VF tracking to monitor track entry 1 and specify the value by which the weight decreases, making the weight of Switch B decrease by more than 245 (250 in this example) when track entry 1 turns to negative. In such a case, another router with a higher weight can take over.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 weight track 1 reduced 250
```

3. Configure Switch C:

# Configure VLAN 2.

```
<SwitchC> system-view
[SwitchC] vlan 2
[SwitchC-vlan2] port gigabitethernet 1/0/5
[SwitchC-vlan2] quit
```

# Configure VRRP to operate in load balancing mode.

```
[SwitchC] vrrp mode load-balance
```

# Create VRRP group 1 and configure its virtual IPv6 addresses as FE80::10 and 1::10.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ipv6 address fe80::3 link-local
[SwitchC-Vlan-interface2] ipv6 address 1::3 64
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

# Set Switch C to operate in preemptive mode and set the preemption delay to five seconds.

```
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

# Enable Switch C to send RA messages, so that hosts on network segment 1::/64 can learn the default gateway address.

```
[SwitchC-Vlan-interface2] undo ipv6 nd ra halt
[SwitchC-Vlan-interface2]  quit
```

# Create track entry 1 to associate with the physical status of VLAN-interface 3 on Switch C. When the track entry becomes negative, it means that the interface fails.

```
[SwitchC] track 1 interface vlan-interface 3
```

# Configure VF tracking to monitor track entry 1 and specify the value by which the weight decreases, making the weight of Switch C decrease by more than 245 (250 in this example) when track entry 1 turns to negative. In such a case, another router with a higher weight can take over.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 weight track 1 reduced 250
```

4. Verify the configuration:

After the configuration, Host A can ping the external network. To verify the configuration, use the **display ipv6 vrrp verbose** command.

# Display the detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 100
     Admin Status   : Up              State        : Master
     Config Pri     : 120             Running Pri  : 120
     Preempt Mode   : Yes             Delay Time   : 5
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::1 (Local, Master)
                      FE80::2 (Backup)
                      FE80::3 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-4011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 255
     Active         : local
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-4012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : FE80::2
    Forwarder 03
     State          : Listening
     Virtual MAC    : 000f-e2ff-4013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 127
     Active         : FE80::3
   Forwarder Weight Track Information:
     Track Object   : 1              State : Positive       Weight Reduced : 250
```

# Display the detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 100
     Admin Status   : Up              State        : Backup
     Config Pri     : 110             Running Pri  : 110
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 2200ms left
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::2 (Local, Backup)
                      FE80::1 (Master)
                      FE80::3 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Listening
     Virtual MAC    : 000f-e2ff-4011 (Learnt)
     Owner ID       : 0000-5e01-1101
     Priority       : 127
     Active         : FE80::1
    Forwarder 02
     State          : Active
     Virtual MAC    : 000f-e2ff-4012 (Owner)
     Owner ID       : 0000-5e01-1103
     Priority       : 255
     Active         : local
    Forwarder 03
     State          : Listening
     Virtual MAC    : 000f-e2ff-4013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 127
     Active         : FE80::3
   Forwarder Weight Track Information:
     Track Object   : 1              State : Positive      Weight Reduced : 250
```

# Display the detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 100
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 4200ms left
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::3 (Local, Backup)
                      FE80::1 (Master)
                      FE80::2 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Listening
     Virtual MAC    : 000f-e2ff-4011 (Learnt)
     Owner ID       : 0000-5e01-1101
     Priority       : 127
     Active         : FE80::1
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-4012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : FE80::2
    Forwarder 03
     State          : Active
     Virtual MAC    : 000f-e2ff-4013 (Owner)
     Owner ID       : 0000-5e01-1105
     Priority       : 255
     Active         : local
   Forwarder Weight Track Information:
     Track Object   : 1              State : Positive       Weight Reduced : 250
```

The output shows that in VRRP group 1, Switch A is the master and Switch B and Switch C are the backups. Each switch has one AVF and two LVFs acting as the backups.

# When VLAN interface 3 on Switch A fails, use the **display vrrp ipv6 verbose** command to display the detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                Adver Timer  : 100
     Admin Status   : Up               State        : Master
     Config Pri     : 120              Running Pri  : 120
     Preempt Mode   : Yes              Delay Time   : 5
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::1 (Local, Master)
                      FE80::2 (Backup)
                      FE80::3 (Backup)
   Forwarder Information: 3 Forwarders 0 Active
     Config Weight  : 255
     Running Weight : 5
    Forwarder 01
     State          : Initialize
     Virtual MAC    : 000f-e2ff-4011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 0
     Active         : FE80::3
    Forwarder 02
     State          : Initialize
     Virtual MAC    : 000f-e2ff-4012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 0
     Active         : FE80::2
    Forwarder 03
     State          : Initialize
     Virtual MAC    : 000f-e2ff-4013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 0
     Active         : FE80::3
   Forwarder Weight Track Information:
     Track Object   : 1              State : Negative       Weight Reduced : 250
```

# Use the **display vrrp ipv6 verbose** command to display the detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                Adver Timer  : 100
     Admin Status   : Up               State        : Backup
     Config Pri     : 100              Running Pri  : 100
     Preempt Mode   : Yes              Delay Time   : 5
     Become Master  : 4200ms left
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::3 (Local, Backup)
                      FE80::1 (Master)
                      FE80::2 (Backup)
   Forwarder Information: 3 Forwarders 2 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-4011 (Take Over)
     Owner ID       : 0000-5e01-1101
     Priority       : 85
     Active         : local
     Redirect Time  : 93 secs
     Time-out Time  : 1293 secs
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-4012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 85
     Active         : FE80::2
    Forwarder 03
     State          : Active
     Virtual MAC    : 000f-e2ff-4013 (Owner)
     Owner ID       : 0000-5e01-1105
     Priority       : 255
     Active         : local
   Forwarder Weight Track Information:
     Track Object   : 1              State : Positive       Weight Reduced : 250
```

The output shows that when VLAN interface 3 on Switch A fails, the weight of the AVF on Switch A decreases to 5, which is lower than the lower limit of failure. All VFs on Switch A turn to initialized state and cannot be used for packet forwarding. The VF corresponding to MAC address 000f-e2ff-4011 on Switch C becomes the AVF, and Switch C takes over Switch A for packet forwarding.

# When the timeout timer (about 1800 seconds) expires, display the detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 100
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 4200ms left
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::3 (Local, Backup)
                      FE80::1 (Master)
                      FE80::2 (Backup)
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-4012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : FE80::2
    Forwarder 03
```

```
     State          : Active
     Virtual MAC    : 000f-e2ff-4013 (Owner)
     Owner ID       : 0000-5e01-1105
     Priority       : 255
     Active         : local
   Forwarder Weight Track Information:
     Track Object   : 1              State : Positive       Weight Reduced : 250
```

The output shows that when the timeout timer expires, the VF corresponding to virtual MAC address 000f-e2ff-4011 is removed, and does not forward the packets destined for the MAC address any more.

# When Switch A fails, use the **display vrrp ipv6 verbose** command to display the detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode       : Load Balance
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 100
     Admin Status   : Up              State        : Master
     Config Pri     : 110             Running Pri  : 110
     Preempt Mode   : Yes             Delay Time   : 5
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::2 (Local, Master)
                      FE80::3 (Backup)
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 02
     State          : Active
     Virtual MAC    : 000f-e2ff-4012 (Owner)
     Owner ID       : 0000-5e01-1103
     Priority       : 255
     Active         : local
    Forwarder 03
     State          : Listening
     Virtual MAC    : 000f-e2ff-4013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 127
     Active         : FE80::3
   Forwarder Weight Track Information:
     Track Object   : 1              State : Positive       Weight Reduced : 250
```

The output shows that when Switch A fails, Switch B becomes the master because its priority is higher than that of Switch C.

Troubleshooting VRRP

The screen frequently displays error prompts.

Analysis

This error is probably caused by:

- Inconsistent configuration of the devices in the VRRP group.
- A device is attempting to send illegitimate VRRP packets.

Solution

- In the first case, modify the configuration.
- In the latter case, resort to non-technical measures.

Multiple masters are present in the same VRRP group.

Analysis

- Multiple masters coexist for a short period: This is normal and requires no manual intervention.
- Multiple masters coexist for a long period: This is because devices in the VRRP group cannot receive VRRP packets, or the received VRRP packets are illegal.

Solution

Ping between these masters, and do the following:

- If the ping fails, check network connectivity.
- If the ping succeeds, check that their configurations are consistent in terms of number of virtual IP addresses, virtual IP addresses, advertisement interval, and authentication.

Frequent VRRP state transition.

Analysis

The VRRP advertisement interval is set too short.

Solution

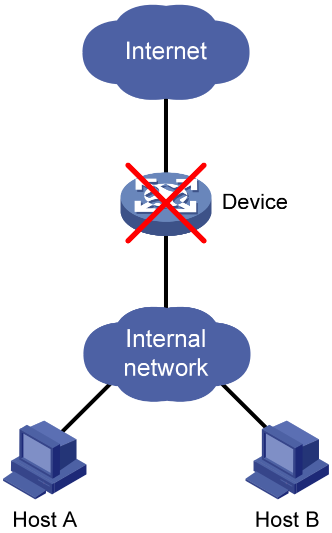
Increase the interval to sent VRRP advertisement or introduce a preemption delay.

Configuring stateful failover (available only on the HP 5500 EI)

Stateful failover overview

Some customers require the key entries or access points of their networks, such as the Internet access point of an enterprise or a database server of a bank, to be highly reliable to ensure continuous data transmission. Deploying only one device (even with high reliability) in such a network risks a single point of failure, as shown in Figure 46. Stateful failover can solve this problem.

Figure 46 Network with one device deployed



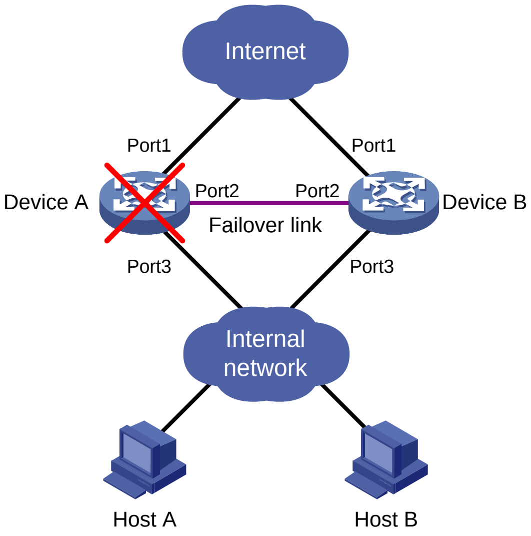
Operating procedure

Stateful failover involves service backup and traffic switchover. The operating procedure of stateful failover is as follows:

1. As shown in Figure 47, Device A and Device B connects to each other over a failover link.
2. The two devices exchange state negotiation messages periodically through the failover link. After the two devices enter the synchronized state, they back up the sessions of each other to make sure that the sessions on them are consistent.
3. If one device fails, the other device can take over the services by using VRRP or a dynamic routing protocol (such as OSPF) to avoid service interruption.

In this document, the stateful failover feature supports backing up only portal services.

Figure 47 Network diagram for stateful failover

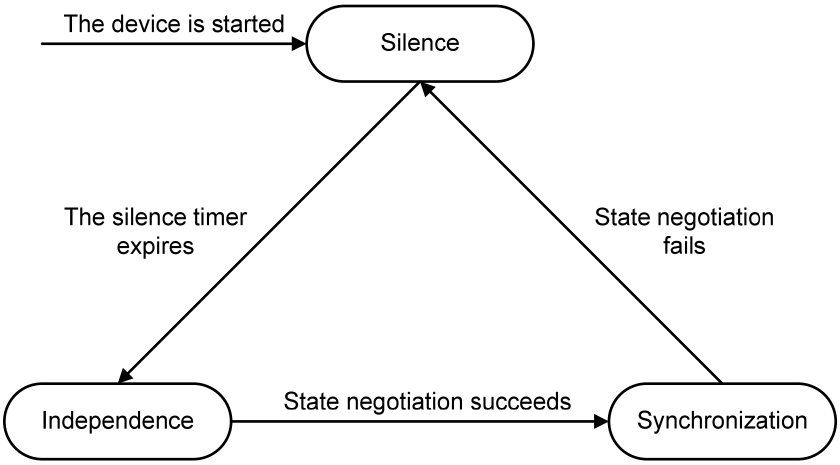


Stateful failover states

Stateful failover has the following states:

- **Silence**—Indicates that the device has just started, or is transiting from synchronization state to independence state.
- **Independence**—Indicates that the silence timer has expired, but no failover link is established.
- **Synchronization**—Indicates that the device has completed state negotiation with the other device and is ready for service backup.

Figure 48 Stateful failover state relations



Introduction to stateful failover configuration

To implement stateful failover on two devices, perform the following configurations:

- Routing configuration. Configure VRRP or a dynamic routing protocol on the devices and the uplink/downlink devices to make sure that the traffic can automatically switch to the other device when a device fails.

- Service backup configuration, which can implement real-time service backup between the two devices.

This configuration guide only introduces the service backup configuration.

Complete the following tasks to configure stateful failover:

Task	Remarks
Enabling stateful failover	Required.
Configuring the backup VLAN	Required.
Service module related configurations	Optional. You must perform further configurations on the device before it can automatically back up portal service information to the backup device. For more information, see *Security Configuration Guide*.

Enabling stateful failover

When you enable stateful failover with the **dhbk enable backup-type** { **dissymmetric-path** | **symmetric-path** } command:

- If you specify the **dissymmetric-path** keyword, the two devices operate in active/active mode. Sessions enter and leave the internal network through different devices to achieve load sharing.
- If you specify the **symmetric-path** keyword, the two devices operate in active/standby mode. Sessions enter and leave the internal network through one device.

Select a keyword based on the network environment and resources, and specify the same keyword for both devices.

To enable stateful failover:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable stateful failover in a specified mode.	**dhbk enable backup-type** { **dissymmetric-path** | **symmetric-path** }	Disabled by default.

Configuring the backup VLAN

After you specify a VLAN as a backup VLAN, the interfaces added to the VLAN can serve as stateful failover interfaces to transmit stateful failover packets.

The device identifies stateful failover packets by the VLAN tag and private protocol number, and broadcasts them in the backup VLAN to the peer. Do not configure other services for the backup VLAN (such as MAC VLAN or Voice VLAN); otherwise, the operation of stateful failover may be affected.

The interfaces assigned to a backup VLAN can forward other packets besides stateful failover packets.

To configure a backup VLAN:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create a VLAN and assign interfaces to the VLAN.	See *Layer 2—LAN Switching Configuration Guide*.	N/A
3.	Return to system view.	**quit**	N/A
4.	Specify the VLAN as a backup VLAN.	**dhbk vlan** *vlan-id*	Not specified by default.

Displaying and maintaining stateful failover

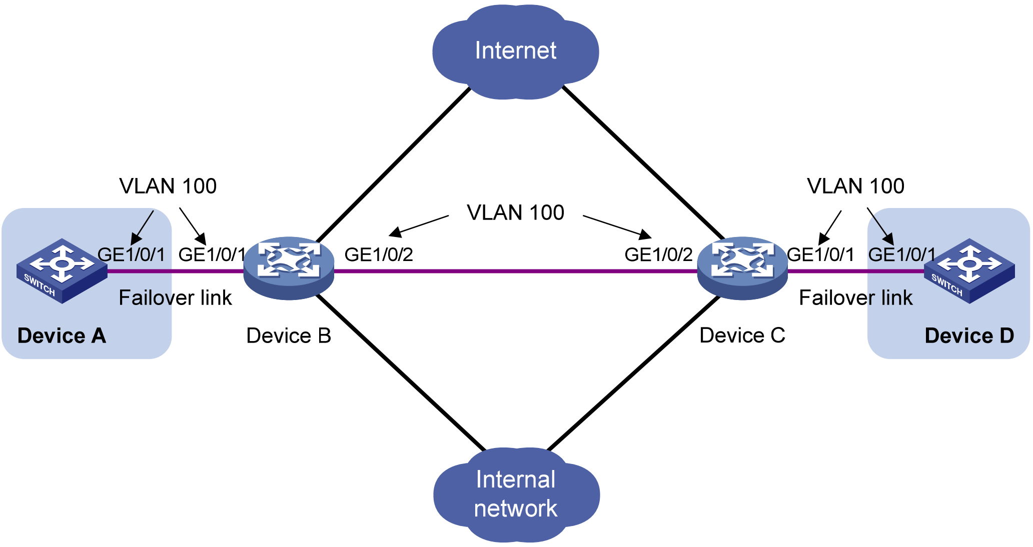
Task	Command	Remarks
Display the running status and related information of stateful failover.	**display dhbk status** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Stateful failover configuration example

Network requirements

In Figure 49, Device B and Device C serve as the internal gateways of an enterprise network. Device A and Device D, respectively attached to Device B and Device C, provide portal access authentication for internal users. Configure stateful failover between Device A and Device D. When one device fails, the other device takes over the services to ensure service continuity.

Figure 49 Network diagram



Configuration procedure

1. Configure Device A:

   # Create VLAN 100.

```
<DeviceA> system-view
```

```
[DeviceA] vlan 100
```

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

```
[DeviceA-vlan100] port gigabitethernet 1/0/1
[DeviceA-vlan100] quit
```

# Specify VLAN 100 as a backup VLAN.

```
[DeviceA] dhbk vlan 100
```

# Enable symmetric-path mode stateful failover.

```
[DeviceA] dhbk enable backup-type symmetric-path
```

2. Configure Device B:

   # Create VLAN 100.

   ```
   <DeviceB> system-view
   [DeviceB] vlan 100
   ```

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

   ```
   [DeviceB-vlan100] port gigabitethernet 1/0/1
   [DeviceB-vlan100] quit
   ```

   # Assign GigabitEthernet 1/0/2 to VLAN 100.

   Because Device B and Device C may exchange packets of multiple VLANs, configure GigabitEthernet 1/0/2 as a trunk port and permit packets of VLAN 100 to pass.

   ```
   [DeviceB] interface gigabitethernet 1/0/2
   [DeviceB-GigabitEthernet1/0/2] port link-type trunk
   [DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 100
    Please wait... Done.
   ```

3. The configurations on Device C are similar to those on Device B. (Details not shown.)
4. The configurations on Device D are similar to those on Device A. (Details not shown.)

Configuration guidelines

When you configure stateful failover, follow these guidelines:

- Stateful failover can be implemented only between two devices rather than among more than two devices.
- The same numbered interfaces must exist on the two devices. Otherwise, session backup fails. For example, if Device A uses GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 to forward backup data, Device B must also use GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3.

Configuring BFD (available only on the HP 5500 EI)

The term *router* in the BFD feature refers to both routers and Layer 3 switches.

The term "interface" in this chapter collectively refers to Layer 3 interfaces, including VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

BFD overview

Devices must quickly detect communication failures so that measures can be taken promptly to ensure service continuity and enhance network availability.

The main fault detection methods include the following:

- **Hardware detection**—Detects link failures by sending hardware detection signals, such as synchronous digital hierarchy (SDH) alarms. Hardware detection can quickly detect link failures, but not all media types support hardware detection.
- **Hello mechanism**—Devices can use the hello mechanism of a routing protocol to detect link failures, which has a failure detection rate in seconds. On a high-speed interface, such as a Gigabit interface, a failure that lasts for one second will cause a large quantity of data to be dropped. The hello mechanism is unacceptable for delay-sensitive services such as voice service. Moreover, this detection method largely relies on the routing protocol.
- **Other detection methods**—Some protocols provide dedicated detection mechanisms. However, they cannot be deployed for inter-system communications.

Bidirectional forwarding detection (BFD) provides a single mechanism to monitor links. With BFD, devices can quickly detect communication failures and restore communications through backup paths.

How BFD works

BFD provides a general-purpose, standard, medium- and protocol-independent fast failure detection mechanism. It can uniformly and quickly detect the failures of the bidirectional forwarding paths between two routers for protocols, such as routing protocols.

BFD provides no neighbor discovery mechanism. Protocols that BFD services notify BFD of routers to which it needs to establish sessions. After a session is established, if no BFD control packet is received from the peer within the negotiated BFD interval, BFD notifies a failure to the protocol, which takes appropriate measures.

Operation of BFD

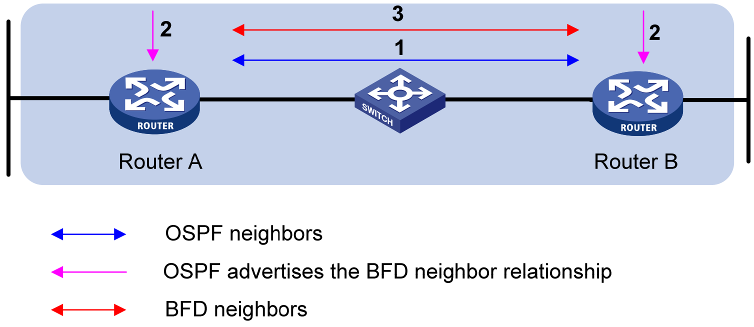


Figure 50 BFD session establishment (on OSPF routers)

The process of BFD session establishment is as follows:

1. A protocol sends hello messages to discover neighbors and establish neighborships.
2. After establishing neighborships, the protocol notifies BFD of the neighbor information, including destination and source addresses.
3. BFD uses the information to establish BFD sessions.

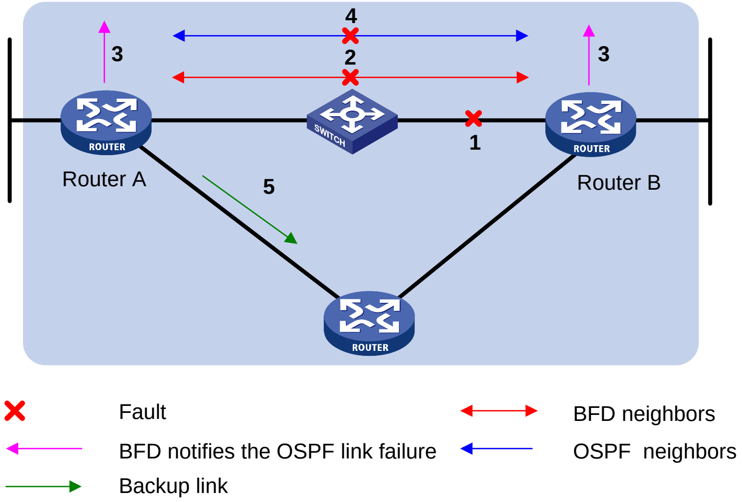


Figure 51 BFD fault detection (on OSPF routers)

The process of BFD fault detection is as follows:

1. BFD detects a link failure.
2. BFD clears the neighbor session.
3. BFD notifies the protocol of the failure.
4. The protocol terminates the neighborship on the link.
5. If a backup link is available, the protocol will use it to forward packets.

NOTE:

No detection time resolution is defined in the BFD draft. Most devices supporting BFD provide detection measured in milliseconds.

BFD detection methods

- **Single-hop detection**—Detects the IP connectivity between two directly connected systems.
- **Multi-hop detection**—Detects any of the paths between two systems. These paths have multiple hops and may be overlapped.
- **Bidirectional detection**—Sends detection packets at two sides of a bidirectional link to detect the bidirectional link status, finding link failures in milliseconds. (BFD LSP detection is a special case in which BFD control packets are sent in one direction, and the peer device reports the link status through other links.)

BFD session modes

- **Control packet mode**—Both ends of the link exchange BFD control packets to monitor link status.
- **Echo mode**—One end of the link sends Echo packets to the other end, which then forwards the packets back to the originating end, monitoring link status in both directions.

BFD operating modes

Before a BFD session is established, BFD has the following operating modes—active and passive.

- **Active mode**—BFD actively sends BFD control packets regardless of whether any BFD control packet is received from the peer.
- **Passive mode**—BFD does not send control packets until a BFD control packet is received from the peer.

At least one end must operate in the active mode for a BFD session to be established.

After a BFD session is established, both ends must operate in the asynchronous mode—Both endpoints periodically send BFD control packets to each other. BFD considers the session down if it receives no BFD control packets within a specific interval.

NOTE:

When a BFD session is maintained by sending Echo packets, the session is independent of the operating mode.

Dynamic BFD parameter changes

After a BFD session is established, both ends can negotiate the related BFD parameters, such as the minimum transmit interval, minimum receive interval, initialization mode, and packet authentication mode. After that, both ends use the negotiated parameters, without affecting the current session state.

Authentication modes

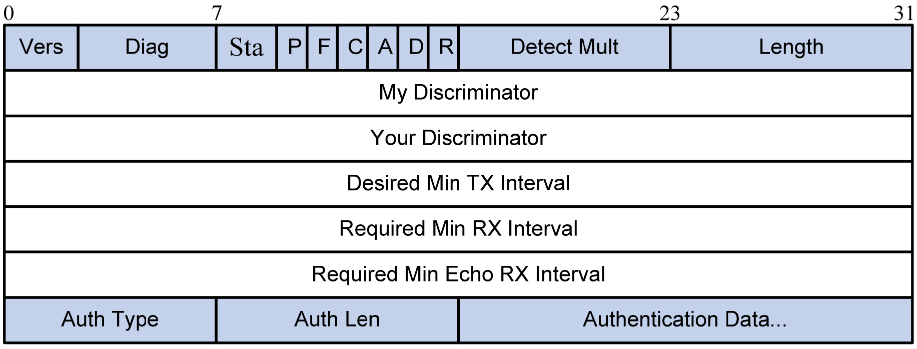
BFD provides the following authentication methods:

- **Simple**—Simple authentication
- **MD5**—MD5 authentication
- **SHA1**—SHA1 authentication

BFD packet format

BFD control packets are encapsulated into UDP packets with port number 3784 for single-hop detection or port number 4784 for multi-hop detection. (It can also be 3784 based on the configuration task.) BFD echo packets have a similar format to BFD control packets (except that the *Desired Min TX Interval* and *Required Min RX Interval* fields are null), with UDP port number 3785.

Figure 52 BFD packet format



- **Vers**—Protocol version. The protocol version is 1.
- **Diag**—This bit indicates the reason for the last transition of the local session from **up** to some other state. Table 19 lists the states.

Table 19 Diag bit values

Diag	Description
0	No Diagnostic
1	Control Detection Time Expired
2	Echo Function Failed
3	Neighbor Signaled Session Down
4	Forwarding Plane Reset
5	Path Down
6	Concatenated Path Down
7	Administratively Down
8	Reverse Concatenated Path Down
9~31	Reserved for future use

- **State (Sta)**—Current BFD session state. Its value can be 0 for AdminDown, 1 for Down, 2 for Init, and 3 for Up.
- **Poll (P)**—If set, the transmitting system is requesting verification of connectivity, or of a parameter change. If clear, the transmitting system is not requesting verification.
- **Final (F)**—If set, the transmitting system is responding to a received BFD control packet that had the Poll (P) bit set. If clear, the transmitting system is not responding to a Poll.
- **Control Plane Independent (C)**—If set, the transmitting system's BFD implementation does not share fate with its control plane (BFD is implemented in the forwarding plane and can continue to function through disruptions in the control plane.) If clear, the transmitting system's BFD implementation shares fate with its control plane.
- **Authentication Present (A)**—If set, the Authentication Section is present, and the session is to be authenticated.
- **Demand (D)**—If set, Demand mode is active in the transmitting system. (The system wishes to operate in Demand mode, knows that the session is up in both directions, and is directing the remote system to cease the periodic transmission of BFD Control packets.) If clear, Demand mode is not active in the transmitting system.

- **Reserved (R)**—This byte must be set to zero on transmit and ignored on receipt.
- **Detect Mult**—Detection time multiplier.
- **Length**—Length of the BFD control packet, in bytes.
- **My Discriminator**—A unique, nonzero discriminator value generated by the transmitting system, used to demultiplex multiple BFD sessions between the same pair of systems.
- **Your Discriminator**—The discriminator received from the remote system. This field reflects back the received value of My Discriminator or is 0 if that value is unknown.
- **Desired Min TX Interval**—This is the minimum interval, in microseconds, that the local system would like to use when transmitting BFD control packets. The value zero is reserved.
- **Required Min RX Interval**—This is the minimum interval, in microseconds, between received BFD control packets that this system is capable of supporting. If this value is zero, the transmitting system does not want the remote system to send any periodic BFD control packets.
- **Required Min Echo RX Interval**—This is the minimum interval, in microseconds, between received BFD echo packets that this system is capable of supporting. If this value is zero, the transmitting system does not support the receipt of BFD echo packets.
- **Auth Type**—The authentication type in use, if the Authentication Present (A) bit is set.
- **Auth Len**—The length, in bytes, of the authentication section, including the Auth Type and Auth Len fields.

Supported features

- OSPF. For more information, see *Layer 3—IP Routing Configuration Guide*.
- OSPFv3. For more information, see *Layer 3—IP Routing Configuration Guide*.
- IS-IS. For more information, see *Layer 3—IP Routing Configuration Guide*.
- IPv6 IS-IS. For more information, see *Layer 3—IP Routing Configuration Guide*.
- RIP. For more information, see *Layer 3—IP Routing Configuration Guide*.
- Static routing. For more information, see *Layer 3—IP Routing Configuration Guide*.
- BGP. For more information, see *Layer 3—IP Routing Configuration Guide*.
- IPv6 BGP. For more information, see *Layer 3—IP Routing Configuration Guide*.
- PIM. For more information, see *IP Multicast Configuration Guide*.
- IPv6 PIM. For more information, see *IP Multicast Configuration Guide*.
- Track. For more information, see "Configuring track."
- IP fast reroute (FRR). Currently, IP FRR is supported by OSPF, RIP, IS-IS, and static routing. For more information, see *Layer 3—IP Routing Configuration Guide*.

Protocols and standards

- RFC 5880, *Bidirectional Forwarding Detection (BFD)*
- RFC 5881, *Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)*
- RFC 5882, *Generic Application of Bidirectional Forwarding Detection (BFD)*
- RFC 5883, *Bidirectional Forwarding Detection (BFD) for Multihop Paths*

Configuring BFD basic functions

The BFD basic functions configuration is the basis for configuring BFD for other protocols.

Configuration prerequisites

Before configuring BFD basic functions, complete the following tasks:

- Configure the network layer addresses of the interfaces so that adjacent nodes are reachable to each other at the network layer
- Configure the routing protocols that support BFD

Configuration procedure

To configure BFD basic functions:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Specify the mode for establishing a BFD session.	**bfd session init-mode** { **active** | **passive** }	Optional. **active** by default.
3.	Configure the destination port number for multi-hop BFD control packets.	**bfd multi-hop destination-port** *port-number*	Optional. 4784 by default.
4.	Configure the source IP address of echo packets.	**bfd echo-source-ip** *ip-address*	Optional. The source IP address should not be on the same network segment as any local interface's IP address. Otherwise, a large number of ICMP redirect packets may be sent from the peer, resulting in link congestion.
5.	Enter interface view.	**interface** *interface-type interface-number*	N/A
6.	Configure the minimum interval for receiving BFD echo packets.	**bfd min-echo-receive-interval** *value*	Optional. For relevant information, see the description of the *Required Min Echo RX Interval* field in "BFD packet format." 400 milliseconds by default.
7.	Configure the minimum interval for transmitting BFD control packets.	**bfd min-transmit-interval** *value*	Optional. For relevant information, see the description of the *Desired Min TX Interval* field in "BFD packet format." 400 milliseconds by default.

Step	Command	Remarks
8. Configure the minimum interval for receiving BFD control packets.	**bfd min-receive-interval** *value*	Optional. For relevant information, see the description of the *Required Min RX Interval* field in "BFD packet format." 400 milliseconds by default.
9. Configure the detection time multiplier.	**bfd detect-multiplier** *value*	Optional. For relevant information, see the description of the *Detect Mult* field in "BFD packet format." 5 by default.
10. Configure the authentication mode on the interface.	**bfd authentication-mode** { **md5** *key-id* [**cipher**] *key* | **sha1** *key-id* [**cipher**] *key* | **simple** *key-id* [**cipher**] *password* }	Optional. By default, the interface operates in the non-authentication mode.

In Figure 50 for example, if you configure the Desired Min TX Interval as 100 milliseconds, Required Min RX Interval as 300 milliseconds, and Detect Mult as 5 on Router A, and configure the Desired Min TX Interval as 150 milliseconds, Required Min RX Interval as 400 milliseconds, and Detect Mult as 10 on Router B,

- The actual transmitting interval on Router A is 400 milliseconds, which is the greater value between the minimum interval for transmitting BFD control packets on Router A (100 milliseconds) and the minimum interval for receiving BFD control packets on Router B (400 milliseconds).
- The actual transmitting interval on Router B is 300 milliseconds, which is the greater value between the minimum interval for transmitting BFD control packets on Router B (150 milliseconds) and the minimum interval for receiving BFD control packets on Router A (300 milliseconds).
- The actual detection time on Router A is 3000 milliseconds, which is 10 × 300 milliseconds (Detect Mult on Router B × actual transmitting interval on Router B).
- The actual detection time on Router B is 2000 milliseconds, which is 5 × 400 milliseconds (Detect Mult on Router A × actual transmitting interval on Router A).

Displaying and maintaining BFD

Task	Command	Remarks
Display information about BFD-enabled interfaces.	**display bfd interface** [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display information about enabled BFD debugging.	**display bfd debugging-switches** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Task	Command	Remarks
Display BFD session information.	**display bfd session** [**slot** *slot-number* [**all** | **verbose**] | **verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear BFD session statistics.	**reset bfd session statistics** [**slot** *slot-number*]	Available in user view

Configuring track

Only the HP 5500 EI Switch Series supports BFD, VRRP, and PBR configurations.

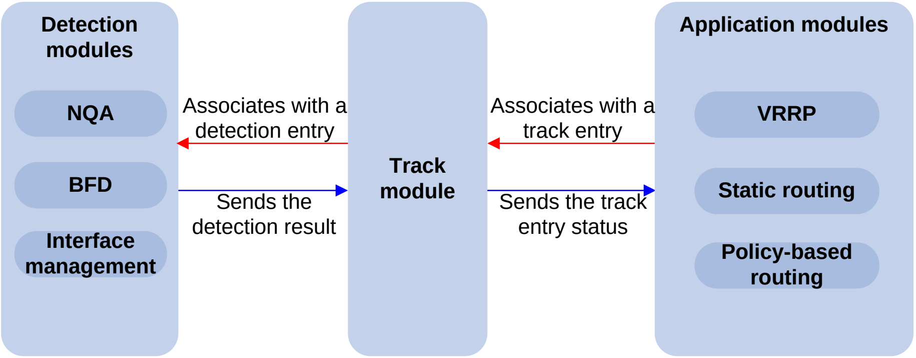
Track overview

Introduction to collaboration

The track module works between application and detection modules, as shown in Figure 53. It shields the differences between various detection modules from application modules.

Collaboration is enabled after you associate the track module with a detection module and an application module. The detection module probes specific objects such as interface status, link status, network reachability, and network performance, and informs the track module of detection results. The track module sends the detection results to the associated application module. When notified of changes of the tracked object, the application modules can react to avoid communication interruption and network performance degradation.

Figure 53 Collaboration through the track module


Detection modules
NQA
BFD
Interface management
Associates with a detection entry
Sends the detection result
Track module
Associates with a track entry
Sends the track entry status
Application modules
VRRP
Static routing
Policy-based routing

Collaboration fundamentals

The track module collaborates with detection modules and application modules:

- Collaboration between the track module and a detection module
- Collaboration between the track module and an application module

Collaboration between the track module and a detection module

The detection module sends the detection result of the associated tracked object to the track module. Depending on the result, the track module changes the status of the track entry:

- If the tracked object functions normally, for example, the target interface is up or the target network is reachable, the state of the track entry is Positive.
- If the tracked object functions abnormally, for example, the target interface is down or the target network is unreachable, the state of the track entry is Negative.

- If the detection result is not valid, for example, the NQA test group that is associated with the track entry does not exist, the state of the track entry is Invalid.

The following detection modules can be associated with the track module:

- NQA
- BFD
- Interface management module

Collaboration between the track module and an application module

After being associated with an application module, when the status of the track entry changes, the track module notifies the application module, which then takes proper actions.

The following application modules can be associated with the track module:

- Virtual Router Redundancy Protocol (VRRP)
- Static routing
- Policy-based routing

In some cases, the status of a track entry changes while a route is still recovering. This leads to problems if the track module immediately notifies the application modules of the status change and the application modules begin using the route before it is ready.

For example, the master in a VRRP group monitors the uplink interface through the track module. When the uplink interface fails, the track module notifies the master to reduce its priority so that a backup with a higher priority can preempt as the master to forward packets. When failed uplink interface recovers, if the track module immediately notifies the original master to restore its priority, the master immediately will forward packets to that interface; however, this result in packet forwarding failure because the uplink route has not yet been recovered.

To solve this problem, configure a delay before the track module notifies the application modules of the track entry status changes.

Collaboration application example

The following is an example of collaboration between NQA, track, and static routing.

Configure a static route with next hop 192.168.0.88 on the device. If the next hop is reachable, the static route is valid. If the next hop becomes unreachable, the static route should become invalid. For this purpose, configure collaboration between the NQA, track, and static routing modules:

1. Create an NQA test group to monitor the reachability of IP address 192.168.0.88.
2. Create a track entry and associate it with the NQA test group. When the next hop 192.168.0.88 is reachable, the track entry is in Positive state. When the next hop becomes unreachable, the track entry is in Negative state.
3. Associate the track entry with the static route. When the track entry turns to the Positive state, the static route is valid. When the associated track entry turns to the Negative state, the static route is invalid.

Track configuration task list

To implement the collaboration function, establish associations between the track module and the detection modules, and between the track module and the application modules.

Complete these tasks to configure the track module:

Task		Remarks
Associating the track module with a detection module	Associating track with NQA	Required. Use any of the approaches.
	Associating track with BFD	
	Associating track with interface management	
Associating the track module with an application module	Associating track with VRRP	Required. Use any of the approaches.
	Associating track with static routing	
	Associating track with PBR	

Associating the track module with a detection module

Associating track with NQA

NQA supports multiple test types to analyze network performance, services, service quality. For example, an NQA test group can periodically detect whether a destination is reachable, or whether the TCP connection to a TCP server can be set up.

An NQA test group functions as follows when it is associated with a track entry:

- If the consecutive failures reach the specified threshold, the NQA module tells the track module that the tracked object malfunctions. Then the track module sets the track entry to the Negative state.
- If the specified threshold is not reached, the NQA module tells the track module that the tracked object functions normally. The track module then sets the track entry to the Positive state.

For more information about NQA, see *Network Management and Monitoring Configuration Guide*.

To associate track with NQA:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create a track entry, associate it with an NQA reaction entry, and specify the delay time for the track module to notify the associated application module when the track entry status changes.	**track** *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]	No track entry is created by default.

NOTE:

If the specified NQA test group or the reaction entry in the track entry does not exist, the status of the track entry is Invalid.

Associating track with BFD

BFD supports the control packet mode and echo mode. Only echo-mode BFD can be associated with a track entry.

The BFD functions as follows when it is associated with a track entry:

- If the BFD detects that the link fails, it informs the track entry of the link failure. The track module then sets the track entry to the Negative state.
- If the BFD detects that the link is normal, the track module sets the track entry to the Positive state.

For more information about BFD, see "Configuring BFD (available only on the HP 5500 EI)."

Configuration prerequisites

Before you associate track with BFD, configure the source address of the BFD echo packets.

Configuration procedure

To associate track with BFD:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create a track entry, associate it with the BFD session, and specify the delay time for the track module to notify the associated application module when the track entry status changes.	**track** *track-entry-number* **bfd echo interface** *interface-type interface-number* **remote ip** *remote-ip* **local ip** *local-ip* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]	No track entry is created by default.

NOTE:

When associating track with BFD, do not configure the virtual IP address of a VRRP group as the local or remote address of a BFD session.

Associating track with interface management

The interface management module monitors the physical status or network-layer protocol status of the interface. The interface management module functions as follows when it is associated with a track entry:

- When the physical or network-layer protocol status of the interface changes to up, the interface management module informs the track module of the change and the track module sets the track entry to Positive.
- When the physical or network-layer protocol status of the interface changes to down, the interface management module informs the track module of the change and the track module sets the track entry to Negative.

To associate track with interface management:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Associate track with interface management.	Create a track entry, associate it with the interface management module to monitor the physical status of an interface, and specify the delay time for the track module to notify the associated application module when the track entry status changes: **track** *track-entry-number* **interface** *interface-type interface-number* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *] Create a track entry, associate it with the interface management module to monitor the Layer 3 protocol status of an interface, and specify the delay time for the track module to notify the associated application module when the track entry status changes: **track** *track-entry-number* **interface** *interface-type interface-number* **protocol** { **ipv4** | **ipv6** } [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]	Use either approach. No track entry is created by default.

Associating the track module with an application module

Associating track with VRRP

VRRP is an error-tolerant protocol. It adds a group of routers that can act as network gateways to a VRRP group, which forms a virtual router. Routers in the VRRP group elect the master acting as the gateway according to their priorities. A router with a higher priority is more likely to become the master. The other routers function as the backups. When the master fails, the backups in the VRRP group elect a new gateway to undertake the responsibility of the failed master. This ensures that the hosts in the network segment can uninterruptedly communicate with external networks.

When VRRP is operating in standard protocol mode or load balancing mode, associate the track module with the VRRP group to implement the following actions:

- Change the priority of a router according to the status of the uplink. If a fault occurs on the uplink of the router, the VRRP group cannot be aware of the uplink failure. If the router is the master, hosts in the LAN cannot access the external network. This problem can be solved by establishing a track-VRRP group association. Use the detection modules to monitor the status of the uplink of the router and establish collaborations between the detection modules, track module and VRRP. When the uplink fails, the detection modules notify the track module to change the status of the monitored track entry to Negative, and the priority of the master then decreases by a specific value, allowing a higher priority router in the VRRP group to become the master, and maintaining proper communication between the hosts in the LAN and the external network.
- Monitor the master on a backup. If a fault occurs on the master, the backup operating in switchover mode will switch to the master immediately to maintain normal communication.

When VRRP is operating in load balancing mode, associate the track module with the VRRP Virtual Forwarder (VF) to implement the following functions:

- Change the priority of the active VF (AVF) according to its uplink state. When the uplink of the AVF fails, the track entry changes to Negative state and the weight of the AVF decreases by a specific value so that the VF with a higher priority becomes the new AVF to forward packets.
- Monitor the AVF status from the listening VF (LVF), which refers to the VF in listening state. When the AVF fails, the LVF that is operating in switchover mode becomes the new AVF to ensure continuous forwarding.

VRRP tracking is not valid on an IP address owner. An IP address owner refers to a router when the IP address of the virtual router is the IP address of an interface on the router in the VRRP group.

For more information about VRRP, see "Configuring VRRP (available only on the HP 5500 EI)."

To associate track with VRRP group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Create a VRRP group and configure its virtual IP address.	**vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*	No VRRP group is created by default.
4. Associate a track entry with a VRRP group.	**vrrp** [**ipv6**] **vrid** *virtual-router-id* **track** *track-entry-number* [**reduced** *priority-reduced* | **switchover**]	No track entry is specified for a VRRP group by default. This command is supported when VRRP is operating in both standard protocol mode and load balancing mode.

To associate track with VRRP VF:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Create a VRRP group and configure its virtual IP address.	**vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*	No VRRP group is created by default.
4. Associate track with VRRP VF.	Associate a track entry with the VRRP VF: **vrrp** [**ipv6**] **vrid** *virtual-router-id* **weight track** *track-entry-number* [**reduced** *weight-reduced*] Configure the LVF to monitor the AVF status through the track entry: **vrrp** [**ipv6**] **vrid** *virtual-router-id* **track** *track-entry-number* **forwarder-switchover member-ip** *ip-address*	Use at least one command. By default, no track entry is specified for a VF. This command is configurable when VRRP is operating in standard mode or load balancing mode. However, this function takes effect only when VRRP is operating in load balancing mode.

NOTE:

- When the status of the track entry changes from Negative to Positive or Invalid, the associated router or VF restores its priority automatically.
- You can associate a nonexistent track entry with a VRRP group or VF. The association takes effect only after you use the **track** command to create the track entry.

Associating track with static routing

A static route is a manually configured route. With a static route configured, packets to the specified destination are forwarded through the path specified by the administrator.

The disadvantage of using static routes is that they cannot adapt to network topology changes. Faults or topological changes in the network can make the routes unreachable, causing network breaks.

To prevent this problem, configure another route to back up the static route. When the static route is reachable, packets are forwarded through the static route. When the static route is unreachable, packets are forwarded through the backup route, avoiding network breaks and enhancing network reliability.

To check the accessibility of a static route in real time, establish association between the track and the static route.

If you specify the next hop but not the egress interface when configuring a static route, you can establish collaborations among the static route, the track module, and detection modules. This enables you to check the accessibility of the static route by the status of the track entry.

- The Positive state of the track entry shows that the next hop of the static route is reachable and that the configured static route is valid.
- The Negative state of the track entry shows that the next hop of the static route is not reachable and that the configured static route is invalid.
- The Invalid state of the track entry shows that the accessibility of the next hop of the static route is unknown and that the static route is valid.

If the track module detects the next hop accessibility of the static route in a private network through NQA, the VPN instance name of the next hop of the static route must be consistent with that configured for the NQA test group. Otherwise, the accessibility detection cannot function properly.

If a static route needs route recursion, the associated track entry must monitor the next hop of the recursive route instead of that of the static route; otherwise, a valid route may be considered invalid.

For more information about static route configuration, see *Layer 3—IP Routing Configuration Guide*.

To associate track with static routing:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Associate the static route with a track entry to check the accessibility of the next hop.	Approach 1: **ip route-static** *dest-address* { *mask* | *mask-length* } { *next-hop-address* | **vpn-instance** *d-vpn-instance-name next-hop-address* } **track** *track-entry-number* [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*] Approach 2: **ip route-static vpn-instance** *s-vpn-instance-name&<1-6> dest-address* { *mask* | *mask-length* } { *next-hop-address* [**public**] **track** *track-entry-number* | **vpn-instance** *d-vpn-instance-name next-hop-address* **track** *track-entry-number* } [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]	Use either approach. Not configured by default. Only the HP 5500 EI Switch Series supports the **vpn-instance** keyword.

NOTE:

You can associate a nonexistent track entry with a static route. The association takes effect only after you use the **track** command to create the track entry.

Associating track with PBR

Policy-based routing (PBR) is a routing mechanism based on user-defined policies. Different from the traditional destination-based routing mechanism, PBR enables you to use a policy (based on the source address and other criteria) to route packets.

PBR cannot detect the availability of any action taken on packets. When an action is not available, packets processed by the action may be discarded. For example, configure PBR to forward packets that match certain criteria through a specific next hop. When the specified next hop fails, PBR cannot sense the failure, and continues to forward matching packets to the next hop.

This problem can be solved by associating track with PBR, which improves the flexibility of PBR application, and enables PBR to sense topology changes.

After you associate a track entry with an apply clause, the detection module associated with the track entry sends the detection result of the availability of the object (an interface or an IP address) specified in the apply clause.

- The Positive state of the track entry shows that the object is available, and the apply clause is valid.
- The Negative state of the track entry shows that the object is not available, and the apply clause is invalid.
- The Invalid state of the track entry shows that the apply clause is valid.

The following objects can be associated with a track entry:

- Next hop
- Default next hop

For more information about PBR, see *Layer 3—IP Routing Configuration Guide*.

Configuration prerequisites

Before you associate track with PBR, create a policy or a policy node and configure the match criteria as well.

Configuration procedure

To associate track with PBR:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create a policy or policy node and enter PBR policy node view.	**policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*	Required.
3.	Define an ACL match criterion.	**if-match acl** *acl-number*	Optional. By default, no packets are filtered.
4.	Associate track with PBR.	Set the next hop and associate it with a track entry: **apply ip-address next-hop** *ip-address* [**direct**] [**track** *track-entry-number*] [*ip-address* [**direct**] [**track** *track-entry-number*]] Set the default next hop, and associate it with a track entry: **apply ip-address default next-hop** *ip-address [* **track** *track-entry-number*] [*ip-address [* **track** *track-entry-number*]]	Configure at least one of the commands.

NOTE:

You can associate a nonexistent track entry with PBR. The association takes effect only after you use the **track** command to create the track entry.

Displaying and maintaining track entries

Task	Command	Remarks
Display information about the specified or all track entries.	**display track** { *track-entry-number* | **all** } [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Track configuration examples

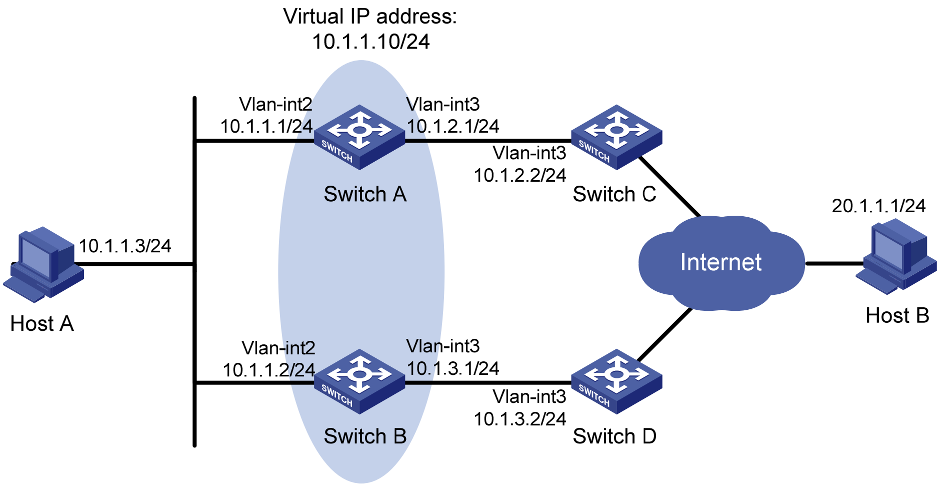
VRRP-track-NQA collaboration configuration example (the master monitors the uplink)

Network requirements

- As shown in Figure 54, Host A needs to access Host B on the Internet. The default gateway of Host A is 10.1.1.10/24.
- Switch A and Switch B belong to VRRP group 1, whose virtual IP address is 10.1.1.10.

- When Switch A operates properly, packets from Host A to Host B are forwarded through Switch A. When VRRP finds that a fault is on the uplink of Switch A through NQA, packets from Host A to Host B are forwarded through Switch B.

Figure 54 Network diagram



Configuration procedure

1. Create VLANs, and assign corresponding ports to the VLANs. Configure the IP address of each VLAN interface as shown in Figure 54. (Details not shown.)
2. Configure an NQA test group on Switch A:

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

# Create an NQA test group with the administrator name **admin** and the operation tag **test**.

```
[SwitchA] nqa entry admin test
```

# Configure the test type as ICMP-echo.

```
[SwitchA-nqa-admin-test] type icmp-echo
```

# Configure the destination address as 10.1.2.2.

```
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.1.2.2
```

# Set the test frequency to 100 ms.

```
[SwitchA-nqa-admin-test-icmp-echo] frequency 100
```

# Configure reaction entry 1, specifying that five consecutive probe failures trigger the track module.

```
[SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail
threshold-type consecutive 5 action-type trigger-only
[SwitchA-nqa-admin-test-icmp-echo] quit
```

# Start the NQA test.

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

3. Configure a track entry on Switch A:

# Configure track entry 1, and associate it with reaction entry 1 of the NQA test group (with the administrator **admin**, and the operation tag **test**).

```
[SwitchA] track 1 nqa entry admin test reaction 1
```

4. Configure VRRP on Switch A:

# Create VRRP group 1, and configure the virtual IP address 10.1.1.10 for the group.

```
[SwitchA] interface vlan-interface 2
```

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

# Set the priority of Switch A in VRRP group 1 to 110.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

# Set the authentication mode of VRRP group 1 to **simple**, and the authentication key to **hello**.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

# Configure the master to send VRRP packets at an interval of five seconds.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

# Configure Switch A to operate in preemptive mode, and set the preemption delay to five seconds.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

# Configure to monitor track entry 1, and specify the priority decrement to 30.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 reduced 30
```

5. Configure VRRP on Switch B:

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
```

# Create VRRP group 1, and configure the virtual IP address 10.1.1.10 for the group.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

# Set the authentication mode of VRRP group 1 to **simple**, and the authentication key to **hello**.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

# Configure the master to send VRRP packets at an interval of five seconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

# Configure Switch B to operate in preemptive mode, and set the preemption delay to five seconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

6. Verify the configuration:

After configuration, ping Host B on Host A, and you can see that Host B is reachable. Use the **display vrrp** command to view the configuration result.

# Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1              Adver Timer  : 5
     Admin Status   : Up             State        : Master
     Config Pri     : 110            Running Pri  : 110
     Preempt Mode   : Yes            Delay Time   : 5
     Auth Type      : Simple         Key          : ******
     Virtual IP     : 10.1.1.10
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 10.1.1.1
   VRRP Track Information:
     Track Object   : 1             State : Positive          Pri Reduced : 30
```

# Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 5
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 2200ms left
     Auth Type      : Simple          Key          : ******
     Virtual IP     : 10.1.1.10
     Master IP      : 10.1.1.1
```

The output shows that in VRRP group 1, Switch A is the master, and Switch B is a backup. Packets from Host A to Host B are forwarded through Switch A.

When a fault is on the link between Switch A and Switch C, you can still successfully ping Host B on Host A. Use the **display vrrp** command to view information about VRRP group 1.

# Display detailed information about VRRP group 1 on Switch A when a fault is on the link between Switch A and Switch C.

```
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 5
     Admin Status   : Up              State        : Backup
     Config Pri     : 110             Running Pri  : 80
     Preempt Mode   : Yes             Delay Time   : 5
     Become Master  : 2200ms left
     Auth Type      : Simple          Key          : ******
     Virtual IP     : 10.1.1.10
     Master IP      : 10.1.1.2
   VRRP Track Information:
     Track Object   : 1              State : Negative          Pri Reduced : 30
```

# Display detailed information about VRRP group 1 on Switch B when a fault is on the link between Switch A and Switch C.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 5
     Admin Status   : Up              State        : Master
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 5
     Auth Type      : Simple          Key          : ******
```

```
Virtual IP     : 10.1.1.10
Virtual MAC    : 0000-5e00-0101
Master IP      : 10.1.1.2
```

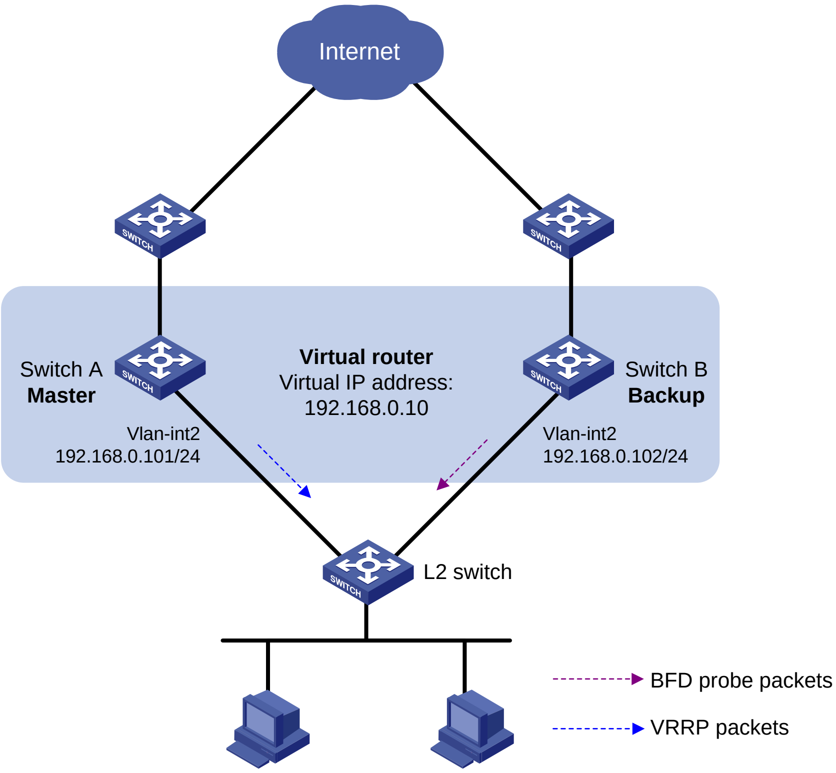
The output shows that when a fault is on the link between Switch A and Switch C, the priority of Switch A decreases to 80. Switch A becomes the backup, and Switch B becomes the master. Packets from Host A to Host B are forwarded through Switch B.

Configuring BFD for a VRRP backup to monitor the master

Network requirements

- As shown in Figure 55, Switch A and Switch B belong to VRRP group 1, whose virtual IP address is 192.168.0.10.
- The default gateway of the hosts in the LAN is 192.168.0.10. When Switch A operates properly, the hosts in the LAN access the external network through Switch A. When Switch A fails, the hosts in the LAN access the external network through Switch B.
- If BFD is not configured, when the master in a VRRP group fails, the backup cannot become the master until the configured timeout timer expires. The timeout is generally three to four seconds, which makes the switchover slow. To solve this problem, VRRP uses BFD to probe the state of the master. Once the master fails, the backup can become the new master in milliseconds.

Figure 55 Network diagram



Configuration procedure

1. Create VLANs, and assign corresponding ports to the VLANs. Configure the IP address of each VLAN interface as shown in Figure 55. (Details not shown.)
2. Configure VRRP on Switch A:

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

```
[SwitchA] interface vlan-interface 2
```

# Create VRRP group 1, and configure the virtual IP address 192.168.0.10 for the group. Set the priority of Switch A in VRRP group 1 to 110.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
[SwitchA-Vlan-interface2] return
```

3. Configure BFD on Switch B:

   # Configure the source address of BFD echo packets as 10.10.10.10.

   ```
   <SwitchB> system-view
   [SwitchB] bfd echo-source-ip 10.10.10.10
   ```

4. Create the track entry to be associated with the BFD session on Switch B:

   # Create track entry 1 to be associated with the BFD session to check whether Switch A is reachable.

   ```
   [SwitchB] track 1 bfd echo interface vlan-interface 2 remote ip 192.168.0.101 local ip 192.168.0.102
   ```

5. Configure VRRP on Switch B:

   # Create VRRP group 1, and configure the virtual IP address 192.168.0.10 for the group. VRRP group 1 monitors the status of track entry 1. When the status of the track entry becomes Negative, Switch B quickly becomes the master.

   ```
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
   [SwitchB-Vlan-interface2] vrrp vrid 1 track 1 switchover
   [SwitchB-Vlan-interface2] return
   ```

6. Verify the configuration:

   # Display the detailed information about VRRP group 1 on Switch A.

   ```
   <SwitchA> display vrrp verbose
    IPv4 Standby Information:
        Run Mode       : Standard
        Run Method     : Virtual MAC
    Total number of virtual routers : 1
      Interface Vlan-interface2
        VRID           : 1               Adver Timer  : 1
        Admin Status   : Up              State        : Master
        Config Pri     : 110             Running Pri  : 110
        Preempt Mode   : Yes             Delay Time   : 0
        Auth Type      : None
        Virtual IP     : 192.168.0.10
        Virtual MAC    : 0000-5e00-0101
        Master IP      : 192.168.0.101
   ```

   # Display the detailed information about VRRP group 1 on Switch B.

   ```
   <SwitchB> display vrrp verbose
    IPv4 Standby Information:
        Run Mode       : Standard
        Run Method     : Virtual MAC
    Total number of virtual routers : 1
      Interface Vlan-interface2
        VRID           : 1               Adver Timer  : 1
   ```

```
     Admin Status   : Up             State        : Backup
     Config Pri     : 100            Running Pri  : 100
     Preempt Mode   : Yes            Delay Time   : 0
     Become Master  : 2200ms left
     Auth Type      : None
     Virtual IP     : 192.168.0.10
     Master IP      : 192.168.0.101
   VRRP Track Information:
     Track Object   : 1              State : Positive          Switchover
```

# Display information about track entry 1 on Switch B.

```
<SwitchB> display track 1
Track ID: 1
  Status: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD session:
    Packet type: Echo
    Interface  : Vlan-interface2
    Remote IP  : 192.168.0.101
    Local IP   : 192.168.0.102
```

The output shows that when the status of the track entry becomes Positive, Switch A is the master, and Switch B the backup.

# Enable VRRP state debugging and BFD event debugging on Switch B.

```
<SwitchB> terminal debugging
<SwitchB> terminal monitor
<SwitchB> debugging vrrp state
<SwitchB> debugging bfd event
```

# When Switch A fails, the following output is displayed on Switch B.

```
*Dec 17 14:44:34:142 2008 SwitchB BFD/7/EVENT:Send sess-down Msg,
[Src:192.168.0.102,Dst:192.168.0.101,Vlan-interface2,Echo], instance:0,
protocol:Track
*Dec 17 14:44:34:144 2008 SwitchB VRRP/7/DebugState: IPv4 Vlan-interface2 | Virtual
Router 1 : Backup --> Master   reason: The status of the tracked object changed
```

# Display the detailed information about the VRRP group on Switch B.

```
<SwitchB> display vrrp verbose
IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1              Adver Timer  : 1
     Admin Status   : Up             State        : Master
     Config Pri     : 100            Running Pri  : 100
     Preempt Mode   : Yes            Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 192.168.0.10
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.102
   VRRP Track Information:
     Track Object   : 1                State : Negative          Switchover
```

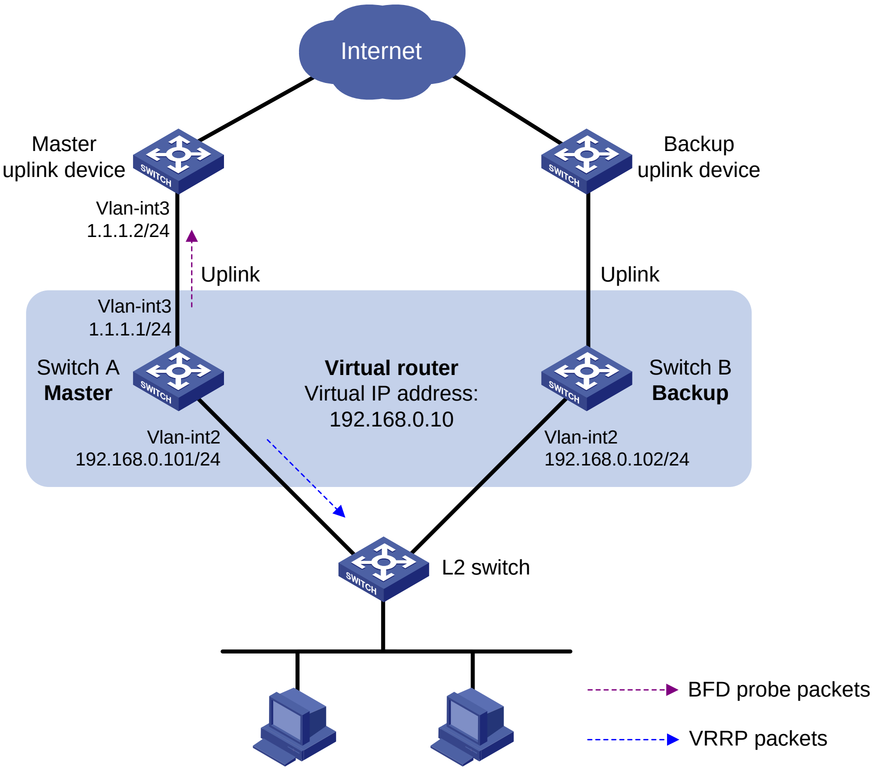
The output shows that when BFD detects that Switch A fails, it notifies VRRP through the track module to change the status of Switch B to master without waiting for a period three times the advertisement interval, so that a backup can quickly preempt as the master.

Configuring BFD for the VRRP master to monitor the uplinks

Network requirements

- As shown in Figure 56, Switch A and Switch B belong to VRRP group 1, whose virtual IP address is 192.168.0.10.
- The default gateway of the hosts in the LAN is 192.168.0.10.
- When Switch A operates properly, the hosts in the LAN access the external network through Switch A. When Switch A detects that the uplink is down through BFD, it decreases its priority so that Switch B can preempt as the master, ensuring that the hosts in the LAN can access the external network through Switch B.

Figure 56 Network diagram



Configuration procedure

1. Create VLANs, and assign corresponding ports to the VLANs. Configure the IP address of each VLAN interface as shown in Figure 56. (Details not shown.)
2. Configure BFD on Switch A:

   # Configure the source address of BFD echo packets as 10.10.10.10.

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

```
[SwitchA] bfd echo-source-ip 10.10.10.10
```

3. Create a track entry to be associated with the BFD session on Switch A:

   # Create track entry 1 to be associated with the BFD session to check whether the uplink device with the IP address 1.1.1.2 is reachable.

```
[SwitchA] track 1 bfd echo interface vlan-interface 3 remote ip 1.1.1.2 local ip
1.1.1.1
```

4. Configure VRRP on Switch A:

   # Create VRRP group 1, and configure the virtual IP address of the group as 192.168.0.10. Configure the priority of Switch A in VRRP group 1 as 110. Configure VRRP group 1 to monitor the status of track entry 1. When the status of the track entry becomes Negative, the priority of Switch A decreases by 20.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 reduced 20
[SwitchA-Vlan-interface2] return
```

5. Configure VRRP on Switch B:

   # Create VRRP group 1, and configure the virtual IP address of the group as 192.168.0.10.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
[SwitchB-Vlan-interface2] return
```

6. Verify the configuration:

   # Display the detailed information about the VRRP group on Switch A.

```
<SwitchA> display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Master
     Config Pri     : 110             Running Pri  : 110
     Preempt Mode   : Yes             Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 192.168.0.10
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.101
   VRRP Track Information:
     Track Object   : 1               State : Positive   Pri Reduced : 20
```

   # Display the information about track entry 1 on Switch A.

```
<SwitchA> display track 1
Track ID: 1
  Status: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD session:
    Packet type: Echo
    Interface  : Vlan-interface2
    Remote IP  : 1.1.1.2
    Local IP   : 1.1.1.1
```

# Display the detailed information about the VRRP group on Switch B.

```
<SwitchB> display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 0
     Become Master  : 2200ms left
     Auth Type      : None
     Virtual IP     : 192.168.0.10
     Master IP      : 192.168.0.101
```

The output shows that when the status of track entry 1 becomes **Positive**, Switch A is the master, and Switch B the backup.

# When the uplink of Switch A goes down, the status of track entry 1 becomes **Negative**.

```
<SwitchA> display track 1
Track ID: 1
  Status: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD session:
    Packet type: Echo
    Interface  : Vlan-interface2
    Remote IP  : 1.1.1.2
    Local IP   : 1.1.1.1
```

# Display the detailed information about VRRP group 1 on Switch A.

```
<SwitchA> display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Backup
     Config Pri     : 110             Running Pri  : 90
     Preempt Mode   : Yes             Delay Time   : 0
     Become Master  : 2200ms left
     Auth Type      : None
     Virtual IP     : 192.168.0.10
     Master IP      : 192.168.0.102
   VRRP Track Information:
     Track Object   : 1                State : Negative   Pri Reduced : 20
```

# Display the detailed information about VRRP group 1 on Switch B.

```
<SwitchB> display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                Adver Timer  : 1
     Admin Status   : Up               State        : Master
     Config Pri     : 100              Running Pri  : 100
     Preempt Mode   : Yes              Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 192.168.0.10
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.102
```

The output shows that when Switch A detects that the uplink fails through BFD, it decreases its priority by 20 to make sure that Switch B can preempt as the master.

Static routing-track-NQA collaboration configuration example

Network requirements

As shown in Figure 57, Switch A, Switch B, Switch C, and Switch D are connected to two segments 20.1.1.0/24 and 30.1.1.0/24. Configure static routes on these switches so that the two segments can communicate with each other, and configure route backup to improve reliability of the network.

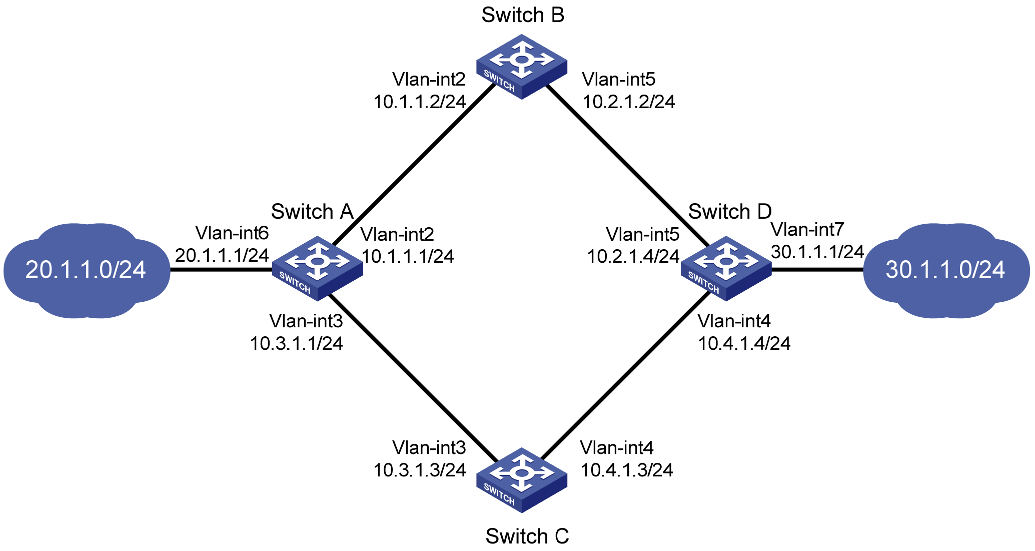
Switch A is the default gateway of the hosts in segment 20.1.1.0/24. Two static routes to 30.1.1.0/24 exist on Switch A, with the next hop being Switch B and Switch C, respectively. These two static routes back up each other as follows:

- The static route with Switch B as the next hop has a higher priority, and is the master route. If this route is available, Switch A forwards packets to 30.1.1.0/24 through Switch B.
- The static route with Switch C as the next hop acts as the backup route.
- Configure static routing-track-NQA collaboration to determine whether the master route is available in real time. If the master route is unavailable, the backup route takes effect, and Switch A forwards packets to 30.1.1.0/24 through Switch C.

Similarly, Switch D is the default gateway of the hosts in segment 30.1.1.0/24. Two static routes to 20.1.1.0/24 exist on Switch D, with the next hop being Switch B and Switch C, respectively. These two static routes back up each other as follows:

- The static route with Switch B as the next hop has a higher priority, and is the master route. If this route is available, Switch D forwards packets to 20.1.1.0/24 through Switch B.
- The static route with Switch C as the next hop acts as the backup route.
- Configure static routing-track-NQA collaboration to determine whether the master route is available in real time. If the master route is unavailable, the backup route takes effect, and Switch D forwards packets to 20.1.1.0/24 through Switch C.

Figure 57 Network diagram



Configuration procedure

1. Create VLANs, and assign corresponding ports to the VLANs. Configure the IP address of each VLAN interface as shown in Figure 57. (Details not shown.)
2. Configure Switch A:

   # Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.1.1.2 and the default priority 60. This static route is associated with track entry 1.

   ```
   <SwitchA> system-view
   [SwitchA] ip route-static 30.1.1.0 24 10.1.1.2 track 1
   ```

   # Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.3.1.3 and the priority 80.

   ```
   [SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
   ```

   # Configure a static route to 10.2.1.4, with the address of the next hop as 10.1.1.2.

   ```
   [SwitchA] ip route-static 10.2.1.4 24 10.1.1.2
   ```

   # Create an NQA test group with the administrator **admin** and the operation tag **test**.

   ```
   [SwitchA] nqa entry admin test
   ```

   # Configure the test type as ICMP-echo.

   ```
   [SwitchA-nqa-admin-test] type icmp-echo
   ```

   # Configure the destination address of the test as 10.2.1.4 and the next hop address as 10.1.1.2 to check the connectivity of the path from Switch A to Switch B and then to Switch D through NQA.

   ```
   [SwitchA-nqa-admin-test-icmp-echo] destination ip 10.2.1.4
   [SwitchA-nqa-admin-test-icmp-echo] next-hop 10.1.1.2
   ```

   # Configure the test frequency as 100 ms.

   ```
   [SwitchA-nqa-admin-test-icmp-echo] frequency 100
   ```

   # Configure reaction entry 1, specifying that five consecutive probe failures trigger the track module.

   ```
   [SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail
   threshold-type consecutive 5 action-type trigger-only
   [SwitchA-nqa-admin-test-icmp-echo] quit
   ```

   # Start the NQA test.

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

# Configure track entry 1, and associate it with reaction entry 1 of the NQA test group (with the administrator **admin**, and the operation tag **test**).

```
[SwitchA] track 1 nqa entry admin test reaction 1
```

3. Configure Switch B:

# Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.2.1.4.

```
<SwitchB> system-view
[SwitchB] ip route-static 30.1.1.0 24 10.2.1.4
```

# Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.1.1.1.

```
[SwitchB] ip route-static 20.1.1.0 24 10.1.1.1
```

4. Configure Switch C:

# Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.4.1.4.

```
<SwitchC> system-view
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.4
```

# Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.3.1.1.

```
[SwitchC] ip route-static 20.1.1.0 24 10.3.1.1
```

5. Configure Switch D:

# Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.2.1.2 and the default priority 60. This static route is associated with track entry 1.

```
<SwitchD> system-view
[SwitchD] ip route-static 20.1.1.0 24 10.2.1.2 track 1
```

# Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.4.1.3 and the priority 80.

```
[SwitchD] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

# Configure a static route to 10.1.1.1, with the address of the next hop as 10.2.1.2.

```
[SwitchD] ip route-static 10.1.1.1 24 10.2.1.2
```

# Create an NQA test group with the administrator **admin** and the operation tag **test**.

```
[SwitchD] nqa entry admin test
```

# Configure the test type as ICMP-echo.

```
[SwitchD-nqa-admin-test] type icmp-echo
```

# Configure the destination address of the test as 10.1.1.1 and the next hop address as 10.2.1.2 to check the connectivity of the path from Switch D to Switch B and then to Switch A through NQA.

```
[SwitchD-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
[SwitchD-nqa-admin-test-icmp-echo] next-hop 10.2.1.2
```

# Configure the test frequency as 100 ms.

```
[SwitchD-nqa-admin-test-icmp-echo] frequency 100
```

# Configure reaction entry 1, specifying that five consecutive probe failures trigger the track module.

```
[SwitchD-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail
threshold-type consecutive 5 action-type trigger-only
[SwitchD-nqa-admin-test-icmp-echo] quit
```

# Start the NQA test.

```
[SwitchD] nqa schedule admin test start-time now lifetime forever
```

# Configure track entry 1, and associate it with reaction entry 1 of the NQA test group (with the administrator **admin**, and the operation tag **test**).

```
[SwitchD] track 1 nqa entry admin test reaction 1
```

6. Verify the configuration:

# Display information about the track entry on Switch A.

```
[SwitchA] display track all
Track ID: 1
  Status: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

# Display the routing table of Switch A.

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 10       Routes : 10
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Static 60   0            10.1.1.2        Vlan2
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 60   0            10.1.1.2        Vlan2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

The output shows the NQA test result: the master route is available (the status of the track entry is Positive), and Switch A forwards packets to 30.1.1.0/24 through Switch B.

# Remove the IP address of interface VLAN-interface 2 on Switch B.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] undo ip address
```

# Display information about the track entry on Switch A.

```
[SwitchA] display track all
Track ID: 1
  Status: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

# Display the routing table of Switch A.

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

         Destinations : 10       Routes : 10
```

```
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Static 60   0            10.1.1.2        Vlan2
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 80   0            10.3.1.3        Vlan3
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

The output shows the NQA test result: the master route is unavailable. (The status of the track entry is Negative.) The backup static route takes effect and Switch A forwards packets to 30.1.1.0/24 through Switch C.

# When the master route fails, the hosts in 20.1.1.0/24 can still communicate with the hosts in 30.1.1.0/24.

```
[SwitchA] ping -a 20.1.1.1 30.1.1.1
  PING 30.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
    Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
    Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
  --- 30.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

# The output on Switch D is similar to that on Switch A. When the master route fails, the hosts in 30.1.1.0/24 can still communicate with the hosts in 20.1.1.0/24.

```
[SwitchB] ping -a 30.1.1.1 20.1.1.1
  PING 20.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
    Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
  --- 20.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

Static routing-Track-BFD collaboration configuration example

Network requirements

As shown in Figure 58, Switch A, Switch B, and Switch C are connected to two segments 20.1.1.0/24 and 30.1.1.0/24. Configure static routes on these routers so that the two segments can communicate with each other, and configure route backup to improve reliability of the network.

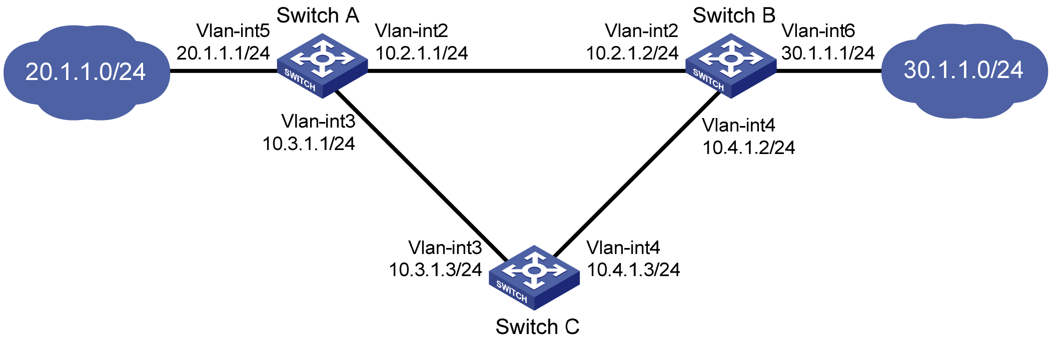
Switch A is the default gateway of the hosts in segment 20.1.1.0/24. Two static routes to 30.1.1.0/24 exist on Switch A, with the next hop being Switch B and Switch C, respectively. These two static routes back up each other as follows:

- The static route with Switch B as the next hop has a higher priority and is the master route. If this route is available, Switch A forwards packets to 30.1.1.0/24 through Switch B.
- The static route with Switch C as the next hop acts as the backup route.
- Configure static routing-track-BFD collaboration to determine whether the master route is available in real time. If the master route is unavailable, BFD can quickly detect the route failure to make the backup route take effect, and Switch A forwards packets to 30.1.1.0/24 through Switch C and Switch B.

Similarly, Switch B is the default gateway of the hosts in segment 30.1.1.0/24. Two static routes to 20.1.1.0/24 exist on Switch B, with the next hop being Switch A and Switch C, respectively. These two static routes back up each other as follows:

- The static route with Switch A as the next hop has a higher priority and is the master route. If this route is available, Switch B forwards packets to 20.1.1.0/24 through Switch A.
- The static route with Switch C as the next hop acts as the backup route.
- Configure static routing-track-BFD collaboration to determine whether the master route is available in real time. If the master route is unavailable, BFD can quickly detect the route failure to make the backup route take effect, and Switch B forwards packets to 20.1.1.0/24 through Switch C and Switch A.

Figure 58 Network diagram



Configuration procedure

1. Create VLANs, and assign corresponding ports to the VLANs. Configure the IP address of each VLAN interface as shown in Figure 58. (Details not shown.)
2. Configure Switch A:

   # Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.2.1.2 and the default priority 60. This static route is associated with track entry 1.

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

```
[SwitchA] ip route-static 30.1.1.0 24 10.2.1.2 track 1
```

# Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.3.1.3 and the priority 80.

```
[SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
```

# Configure the source address of BFD echo packets as 10.10.10.10.

```
[SwitchA] bfd echo-source-ip 10.10.10.10
```

# Configure track entry 1, and associate it with the BFD session. Check whether Switch A can be interoperated with the next hop of static route (Switch B).

```
[SwitchA] track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.2 local ip
10.2.1.1
```

3. Configure Switch B:

# Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.2.1.1 and the default priority 60. This static route is associated with track entry 1.

```
<SwitchB> system-view
[SwitchB] ip route-static 20.1.1.0 24 10.2.1.1 track 1
```

# Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.4.1.3 and the priority 80.

```
[SwitchB] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

# Configure the source address of BFD echo packets as 1.1.1.1.

```
[SwitchB] bfd echo-source-ip 1.1.1.1
```

# Configure track entry 1 that is associated with the BFD session to check whether Switch B can communicate with the next hop (Switch A) of the static route.

```
[SwitchB] track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.1 local ip
10.2.1.2
```

4. Configure Switch C:

# Configure a static route to 30.1.1.0/24, with the address of the next hop as 10.4.1.2.

```
<SwitchC> system-view
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.2
```

# Configure a static route to 20.1.1.0/24, with the address of the next hop as 10.3.1.1.

```
[SwitchB] ip route-static 20.1.1.0 24 10.3.1.1
```

5. Verify the configuration:

# Display information about the track entry on Switch A.

```
[SwitchA] display track all
Track ID: 1
  Status: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD Session:
    Packet type: Echo
    Interface  : Vlan-interface2
    Remote IP  : 10.2.1.2
    Local IP   : 10.2.1.1
```

# Display the routing table of Switch A.

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

```
         Destinations : 9        Routes : 9
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.2.1.0/24         Direct 0    0            10.2.1.1        Vlan2
10.2.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan5
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 60   0            10.2.1.2        Vlan2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

The output shows the BFD detection result: the next hop 10.2.1.2 is reachable. (The status of the track entry is Positive.) The master static route takes effect. Switch A forwards packets to 30.1.1.0/24 through Switch B.

# Remove the IP address of interface VLAN-interface 2 on Switch B.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] undo ip address
```

# Display information about the track entry on Switch A.

```
[SwitchA] display track all
Track ID: 1
  Status: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD Session:
    Packet type: Echo
    Interface  : Vlan-interface2
    Remote IP  : 10.2.1.2
    Local IP   : 10.2.1.1
```

# Display the routing table of Switch A.

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 9        Routes : 9
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.2.1.0/24         Direct 0    0            10.2.1.1        Vlan2
10.2.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan5
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 80   0            10.3.1.3        Vlan3
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

The output shows the BFD detection result: the next hop 10.2.1.2 is unreachable (the status of the track entry is Negative), and the backup static route takes effect, and Switch A forwards packets to 30.1.1.0/24 through Switch C and Switch B.

# When the master route fails, the hosts in 20.1.1.0/24 can still communicate with the hosts in 30.1.1.0/24.

```
[SwitchA] ping -a 20.1.1.1 30.1.1.1
  PING 30.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
    Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
    Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
  --- 30.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

# The output on Switch B is similar to that on Switch A. When the master route fails, the hosts in 30.1.1.0/24 can still communicate with the hosts in 20.1.1.0/24.

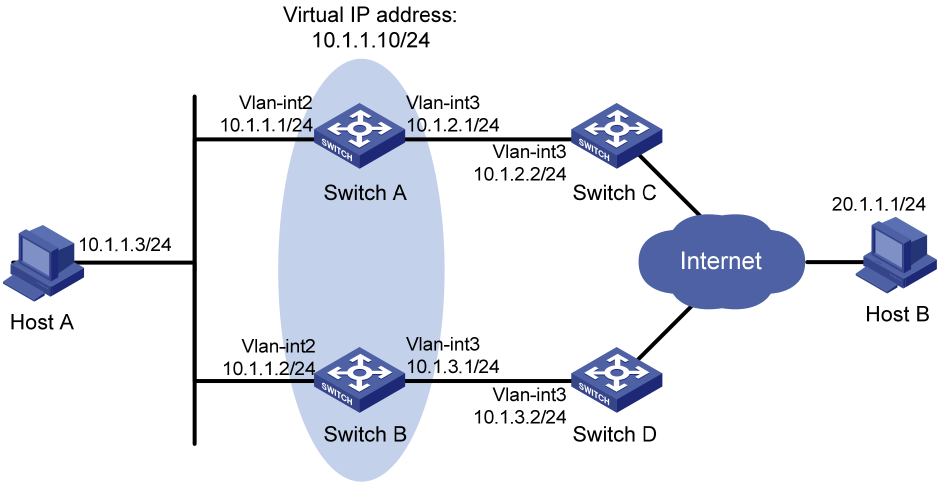
```
[SwitchB] ping -a 30.1.1.1 20.1.1.1
  PING 20.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
    Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms
  --- 20.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

VRRP-track-interface management collaboration configuration example (the master monitors the uplink interface)

Network requirements

- As shown in Figure 59, Host A needs to access Host B on the Internet. The default gateway of Host A is 10.1.1.10/24.
- Switch A and Switch B belong to VRRP group 1, whose virtual IP address is 10.1.1.10.
- When Switch A operates properly, packets from Host A to Host B are forwarded through Switch A. When VRRP detects that a fault is on the uplink interface of Switch A through the interface management module, packets from Host A to Host B are forwarded through Switch B.

Figure 59 Network diagram



Configuration procedure

1. Create VLANs, and assign corresponding ports to the VLANs. Configure the IP address of each VLAN interface as shown in Figure 59. (Details not shown.)
2. Configure a track entry on Switch A:

   # Configure track entry 1, and associate it with the physical status of the uplink interface VLAN-interface 3.

   ```
   [SwitchA] track 1 interface vlan-interface 3
   ```
3. Configure VRRP on Switch A:

   # Create VRRP group 1, and configure the virtual IP address 10.1.1.10 for the group.

   ```
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
   ```

   # Set the priority of Switch A in VRRP group 1 to 110.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
   ```

   # Configure to monitor track entry 1, and specify the priority decrement as 30.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 track 1 reduced 30
   ```
4. Configure VRRP on Switch B:

   ```
   <SwitchB> system-view
   [SwitchB] interface vlan-interface 2
   ```

   # Create VRRP group 1, and configure the virtual IP address 10.1.1.10 for the group.

   ```
   [SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
   ```
5. Verify the configuration:

   After configuration, ping Host B on Host A, and you can see that Host B is reachable. Use the **display vrrp** command to view the configuration result.

   # Display detailed information about VRRP group 1 on Switch A.

   ```
   [SwitchA-Vlan-interface2] display vrrp verbose
    IPv4 Standby Information:
        Run Mode       : Standard
        Run Method     : Virtual MAC
    Total number of virtual routers : 1
      Interface Vlan-interface2
   ```

```
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Master
     Config Pri     : 110             Running Pri  : 110
     Preempt Mode   : Yes             Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 10.1.1.10
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 10.1.1.1
   VRRP Track Information:
     Track Object   : 1               State : Positive   Pri Reduced : 30
```

# Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Backup
     Config Pri     : 100             Running Pri  : 100
     Preempt Mode   : Yes             Delay Time   : 0
     Become Master  : 2200ms left
     Auth Type      : None
     Virtual IP     : 10.1.1.10
     Master IP      : 10.1.1.1
```

The output shows that in VRRP group 1, Switch A is the master, and Switch B is a backup. Packets from Host A to Host B are forwarded through Switch A.

# Shut down the uplink interface VLAN-interface 3 on Switch A.

```
[SwitchA-Vlan-interface2] interface vlan-interface 3
[SwitchA-Vlan-interface3] shutdown
```

After shutting down the uplink interface on Switch A, you can still successfully ping Host B on Host A. Use the **display vrrp** command to view information about VRRP group 1.

# After shutting down the uplink interface on Switch A, display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface3] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1               Adver Timer  : 1
     Admin Status   : Up              State        : Backup
     Config Pri     : 110             Running Pri  : 80
     Preempt Mode   : Yes             Delay Time   : 0
     Become Master  : 2200ms left
     Auth Type      : None
     Virtual IP     : 10.1.1.10
     Master IP      : 10.1.1.2
   VRRP Track Information:
     Track Object   : 1                State : Negative   Pri Reduced : 30
```

# After shutting down the uplink interface on Switch A, display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                Adver Timer  : 1
     Admin Status   : Up               State        : Master
     Config Pri     : 100              Running Pri  : 100
     Preempt Mode   : Yes              Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 10.1.1.10
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 10.1.1.2
```

The output shows that when the uplink interface on Switch A is shut down, the priority of Switch A decreases to 80. Switch A becomes the backup, and Switch B becomes the master. Packets from Host A to Host B are forwarded through Switch B.

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/wwalerts

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Websites

- HP.com http://www.hp.com
- HP Networking http://www.hp.com/go/networking
- HP manuals http://www.hp.com/support/manuals
- HP download drivers and software http://www.hp.com/support/downloads
- HP software depot http://www.software.hp.com
- HP Education http://www.hp.com/learn

Conventions

This section describes the conventions used in this documentation set.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk-marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x | y | ...] *	Asterisk-marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

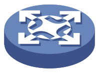
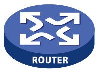
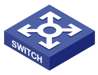
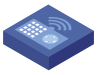
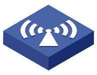
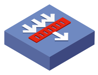
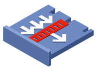
GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in bold text. For example, the **New User** window appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
⚠ WARNING	An alert that calls attention to important information that if not understood or followed can result in personal injury.
△ CAUTION	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
❗ IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
💡 TIP	An alert that provides helpful information.

Network topology icons

	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the switching engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a security product, such as a firewall, a UTM, or a load-balancing or security card that is installed in a device.
	Represents a security card, such as a firewall card, a load-balancing card, or a NetStream card.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index