The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.


Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft® and Windows® are trademarks of the Microsoft group of companies.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.
Contents

High availability overview ........................................................................................................ 1
  Availability requirements ................................................................................................. 1
  Availability evaluation ..................................................................................................... 1
  High availability technologies ........................................................................................ 2
    Fault detection technologies ......................................................................................... 2
    Protection switchover technologies ......................................................................... 2
Configuring Ethernet OAM ................................................................................................. 4
  Overview .......................................................................................................................... 4
    Major functions of Ethernet OAM ................................................................................. 4
    Ethernet OAMPDUs ...................................................................................................... 4
    How Ethernet OAM works .......................................................................................... 4
    Protocols and standards ............................................................................................... 6
  Ethernet OAM configuration task list ............................................................................. 7
  Configuring basic Ethernet OAM functions ................................................................... 7
  Configuring the Ethernet OAM connection detection timers ......................................... 7
  Configuring link monitoring .............................................................................................
    Configuring errored symbol event detection ............................................................ 8
    Configuring errored frame event detection ............................................................... 8
    Configuring errored frame period event detection .................................................. 9
    Configuring errored frame seconds event detection ............................................... 10
  Configuring the action a port takes after it receives an Ethernet OAM event from the remote end ................................................................. 11
  Configuring Ethernet OAM remote loopback ................................................................
    Configuration restrictions and guidelines ................................................................ 12
    Enabling Ethernet OAM remote loopback for a port in system view ...................... 12
    Enabling Ethernet OAM remote loopback for a port in port view ......................... 13
    Rejecting the Ethernet OAM remote loopback request from a remote port .......... 13
  Displaying and maintaining Ethernet OAM ................................................................. 13
  Ethernet OAM configuration example .......................................................................... 14
    Network requirements ................................................................................................. 14
    Configuration procedure ............................................................................................. 14
Configuring CFD .................................................................................................................. 16
  Overview .......................................................................................................................... 16
    Basic CFD concepts ...................................................................................................... 16
    CFD functions .............................................................................................................. 18
    EAIS .............................................................................................................................. 20
    Protocols and standards ............................................................................................... 20
  Configuration restrictions and guidelines ..................................................................... 20
  CFD configuration task list ............................................................................................. 20
  Configuring basic CFD settings ...................................................................................... 21
    Enabling CFD .............................................................................................................. 21
    Configuring Ethernet service instances .................................................................. 21
    Configuring MEPs ........................................................................................................ 22
    Configuring MIP auto-generation rules ...................................................................... 22
  Configuring CFD functions .............................................................................................
    Configuration prerequisites ....................................................................................... 23
    Configuring CC ........................................................................................................... 23
    Configuring LB ............................................................................................................. 24
    Configuring LT ............................................................................................................... 24
    Configuring AIS ........................................................................................................... 25
    Configuring LM ............................................................................................................ 25
    Configuring one-way DM ............................................................................................. 26
    Configuring two-way DM .............................................................................................. 26
    Configuring TST ............................................................................................................. 26
    Configuring EAIS ......................................................................................................... 27
  Displaying and maintaining CFD .................................................................................... 27
## Configuring ERPS

- Overview .................................................................................................................. 96
- ERPS structure ........................................................................................................... 96
- ERPS protocol packets ............................................................................................... 97
- ERPS node states ......................................................................................................... 98
- ERPS timers ................................................................................................................ 98
- ERPS operation mechanism ....................................................................................... 99
- ERPS network diagrams ........................................................................................... 101
- Protocols and standards ............................................................................................. 103
- ERPS configuration task list ....................................................................................... 103
- Configuration prerequisites ......................................................................................... 104
- Enabling ERPS globally ............................................................................................... 104
- Enabling flush packet transparent transmission ......................................................... 104
- Configuring an ERPS ring ........................................................................................... 105
- Enabling R-APS packets to carry the ring ID in the destination MAC address .......... 105
- Configuring ERPS ring member ports ..................................................................... 105

## Configuring RRPP

- Overview .................................................................................................................. 52
- Basic RRPP concepts .................................................................................................. 52
- RRPPDUs .................................................................................................................... 54
- RRPP timers ............................................................................................................... 55
- How RRPP works ....................................................................................................... 55
- Typical RRPP networking ........................................................................................... 56
- Protocols and standards ............................................................................................. 59
- RRPP configuration task list ....................................................................................... 60
- Creating an RRPP domain ........................................................................................... 60
- Configuring control VLANs ....................................................................................... 60
- Configuring protected VLANs ................................................................................... 61
- Configuring RRPP rings ............................................................................................. 62
  - Configuring RRPP ports ........................................................................................... 62
  - Configuring RRPP nodes ........................................................................................ 63
- Activating an RRPP domain ....................................................................................... 64
- Configuring RRPP timers ........................................................................................... 65
- Configuring an RRPP ring group ................................................................................ 65
- Enabling SNMP notifications for RRPP ...................................................................... 66
- Displaying and maintaining RRPP ............................................................................. 66
- RRPP configuration examples ................................................................................... 66
  - Single ring configuration example .......................................................................... 66
  - Intersecting ring configuration example ................................................................... 69
  - Dual-homed rings configuration example ............................................................... 75
  - Load-balanced intersecting-ring configuration example ......................................... 85
- Troubleshooting RRPP ............................................................................................... 95

## Configuring DLDP

- Overview .................................................................................................................. 34
- How DLDP works ....................................................................................................... 35
- Enabling DLDP ........................................................................................................... 39
- Setting the interval to send advertisement packets .................................................... 39
- Setting the DelayDown timer .................................................................................. 39
- Setting the port shutdown mode ................................................................................ 39
- Configuring DLDP authentication ............................................................................. 40
- Displaying and maintaining DLDP ............................................................................ 40
- Configuring DLDP authentication ............................................................................. 40
  - Configuring the auto port shutdown mode ............................................................ 41
  - Configuring the manual port shutdown mode ....................................................... 44
  - Configuring the hybrid port shutdown mode ......................................................... 48

## Configuring DLDP

- Configuration restrictions and guidelines ................................................................ 38
- DLDP configuration task list ..................................................................................... 38
- Setting the port shutdown mode ................................................................................ 39
- Setting the DelayDown timer .................................................................................. 39
- Setting the interval to send advertisement packets .................................................... 39
- Creating an RRPP domain ........................................................................................... 60
- Configuring RRPP nodes ........................................................................................... 63
- Configuring RRPP ports ........................................................................................... 62

## Protocols and Standards

- Basic RRPP concepts .................................................................................................. 52
- Configuring DLDP authentication ............................................................................. 40
- Configuring an RRPP ring group ................................................................................ 65
- Troubleshooting RRPP ............................................................................................... 95
Support and other resources ................................. 291
  Accessing Hewlett Packard Enterprise Support .................................................. 291
  Accessing updates .......................................................... 291
  Websites ................................................................. 292
  Customer self repair ...................................................... 292
  Remote support .......................................................... 292
  Documentation feedback ......................................................... 292

Index ................................................................. 294
High availability overview

Because communication interruptions can seriously affect widely-deployed value-added services such as IPTV and video conference, 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

Table 1 describes a typical availability model that divides availability requirements into different levels.

Table 1 Availability requirements

<table>
<thead>
<tr>
<th>Level</th>
<th>Requirement</th>
<th>Solution</th>
</tr>
</thead>
</table>
| 1     | Decrease system software and hardware faults    | • **Hardware**—Simplified circuit design, enhanced production techniques, and reliability tests.  
|       |                                                 | • **Software**—Reliability design and test. |  
| 2     | Protect system functions from being affected if faults occur | Device and link redundancy and switchover. |
| 3     | Enable the system to recover as fast as possible | Performing fault detection, diagnosis, isolation, and recovery technologies. |

Consider level 1 availability requirements during the design and production processes of network devices.

Consider level 2 availability requirements during network design.

Consider level 3 availability requirements 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.

\[ MTTR = \text{fault detection time} + \text{hardware replacement time} + \text{system initialization time} + \text{link recovery time} + \text{routing time} + \text{forwarding recovery time}. \]

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 in the aspect of 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:

- 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.
- Track works along with other high availability technologies to detect faults through a collaboration mechanism.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Introduction</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLDP</td>
<td>DLDP deals with unidirectional links that might occur in a network. When detecting a unidirectional link, DLDP, as configured, can shut down the related port automatically or prompt users to take actions to avoid network problems.</td>
<td>&quot;Configuring DLDP&quot;</td>
</tr>
<tr>
<td>Ethernet OAM</td>
<td>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 the two devices.</td>
<td>&quot;Configuring Ethernet OAM&quot;</td>
</tr>
<tr>
<td>BFD</td>
<td>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.</td>
<td>&quot;Configuring BFD&quot;</td>
</tr>
<tr>
<td>Monitor Link</td>
<td>Monitor Link associates the state of downlink interfaces with the state of uplink interfaces in a monitor link group. When Monitor Link shuts down the downlink interfaces because of an uplink failure, the downstream device changes connectivity to another link.</td>
<td>&quot;Configuring Monitor Link&quot;</td>
</tr>
<tr>
<td>Track</td>
<td>The Track module implements collaboration between different modules. The collaboration involves three sets of modules: application, Track, and detection. These modules collaborate with one another through collaboration entries. The detection modules trigger the application modules to perform certain operations through the Track module. The detection modules probe such items as link status and network performance, and inform the application modules of the detection result through the Track module. Once notified of network status changes, the application modules use the changes to avoid communication interruption and network performance degradation.</td>
<td>&quot;Configuring Track&quot;</td>
</tr>
</tbody>
</table>

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.
A single availability technology cannot solve all problems. You should use a combination of availability technologies, chosen on the basis of detailed analysis of network environments and user requirements, 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. Network availability should be considered during the planning stage.

Table 3 Protection switchover technologies

<table>
<thead>
<tr>
<th>Technology</th>
<th>Introduction</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active and standby switchover</td>
<td>When a device has two MPUs installed, one MPU is the active MPU, and the other is the standby MPU. Only the active MPU forwards packets and processes services. Typically the system selects the MPU with a smaller slot number as the active MPU. The standby MPU keeps consistent configurations with those on the active MPU through the synchronization function. When the active MPU fails or is removed, the standby MPU automatically becomes the active MPU to ensure non-stop operating of the devices.</td>
<td>N/A</td>
</tr>
<tr>
<td>Ethernet link aggregation</td>
<td>Ethernet link aggregation, or 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.</td>
<td>Layer 2—LAN Switching Configuration Guide</td>
</tr>
<tr>
<td>Smart Link</td>
<td>Smart Link provides link redundancy and fast convergence in a dual uplink network, allowing the backup link to take over quickly when the primary link fails.</td>
<td>“Configuring Smart Link”</td>
</tr>
<tr>
<td>MSTP</td>
<td>As a Layer 2 management protocol, MSTP eliminates Layer 2 loops by selectively blocking redundant links in a network, and in the meantime, allows for link redundancy.</td>
<td>Layer 2—LAN Switching Configuration Guide</td>
</tr>
<tr>
<td>RRPP</td>
<td>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.</td>
<td>“Configuring RRPP”</td>
</tr>
<tr>
<td>ERPS</td>
<td>Ethernet Ring Protection Switching (ERPS) is a robust link layer protocol that ensures a loop-free topology and implements quick link recovery.</td>
<td>“Configuring ERPS”</td>
</tr>
<tr>
<td>GR</td>
<td>GR prevents forwarding discontinuity caused by a protocol restart (including a BGP, IS-IS, OSPF, or LDP) or an active/standby switchover. This feature requires the peer devices to implement routing information backup and recovery.</td>
<td>Related chapters in Layer 3—IP Routing Configuration Guide and MPLS Configuration Guide</td>
</tr>
<tr>
<td>VRRP</td>
<td>VRRP is an error-tolerant protocol, which provides highly reliable default links on multicast and broadcast LANs such as Ethernet, avoiding network interruption due to failure of a single link.</td>
<td>“Configuring VRRP”</td>
</tr>
</tbody>
</table>
Configuring 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." Ethernet OAM improves Ethernet management and maintainability. 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 operates 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 include the following types shown in Table 4.

**Table 4 Functions of different types of OAMPDUs**

<table>
<thead>
<tr>
<th>OAMPDU type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information OAMPDU</td>
<td>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.</td>
</tr>
<tr>
<td>Event Notification OAMPDU</td>
<td>Used by link monitoring to notify the remote OAM entity when it detects problems on the link in between.</td>
</tr>
<tr>
<td>Loopback Control OAMPDU</td>
<td>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.</td>
</tr>
</tbody>
</table>

**NOTE:**
Throughout this document, an Ethernet OAM-enabled port is called an Ethernet OAM entity or an 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 the remote OAM entity to establish a session.

In this phase, two connected OAM entities exchange Information OAMPDUs to advertise their OAM configuration and capabilities to each other for a comparison. If their remote loopback, link detection, and link event settings match, the OAM entities establish an OAM connection.

An OAM entity operates in active mode or passive mode. OAM entities in active mode initiate OAM connections, and OAM entities in passive mode wait and respond to the OAM connection requests. To set up an OAM connection between two OAM entities, you must set at least one entity to operate in active mode.

Table 5 shows the actions that a device can perform in different modes.

Table 5 Active Ethernet OAM mode and passive Ethernet OAM mode

<table>
<thead>
<tr>
<th>Item</th>
<th>Active Ethernet OAM mode</th>
<th>Passive Ethernet OAM mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiating OAM Discovery</td>
<td>Available</td>
<td>Unavailable</td>
</tr>
<tr>
<td>Responding to OAM Discovery</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Transmitting Information OAMPDUs</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Transmitting Event Notification OAMPDUs</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Transmitting Information OAMPDUs without any TLV</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Transmitting Loopback Control OAMPDUs</td>
<td>Available when both sides are operating in active OAM mode</td>
<td>Available</td>
</tr>
<tr>
<td>Responding to Loopback Control OAMPDUs</td>
<td>Available when both sides are operating in active OAM mode</td>
<td>Available</td>
</tr>
</tbody>
</table>

After an Ethernet OAM connection is established, the Ethernet OAM entities exchange Information OAMPDUs at the handshake packet transmission interval to detect the availability of the Ethernet OAM connection. 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 detects link faults in various environments. Ethernet OAM entities monitor link status by exchanging Event Notification OAMPDUs. When detecting one of the link error events listed in Table 6, an OAM entity sends an Event Notification OAMPDU to its peer OAM entity. The network administrator can keep track of network status changes by retrieving the log.

Table 6 Ethernet OAM link error events

<table>
<thead>
<tr>
<th>Ethernet OAM link events</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errored symbol event</td>
<td>An errored symbol event occurs when the number of detected symbol errors in the detection window (specified number of received symbols) exceeds the predefined threshold.</td>
</tr>
<tr>
<td>Errored frame event</td>
<td>An errored frame event occurs when the number of detected error frames in the detection window (specified detection interval) exceeds the predefined threshold.</td>
</tr>
<tr>
<td>Ethernet OAM link events</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Errored frame period event</td>
<td>An errored frame period event occurs when the number of frame errors in the detection window (specified number of received frames) exceeds the predefined threshold.</td>
</tr>
<tr>
<td>Errored frame seconds event</td>
<td>An errored frame seconds event occurs when the number of errored frame seconds (the second in which an errored frame appears is called an errored frame second) detected on a port in the detection window (specified detection interval) reaches the predefined threshold.</td>
</tr>
</tbody>
</table>

Remote fault detection

Information OAMPDUs are exchanged periodically among Ethernet OAM entities across established OAM connections. When traffic is interrupted due to device failure or unavailability, the Ethernet OAM entity at the faulty end sends error information to its peer. The Ethernet OAM entity uses the flag field in Information OAMPDUs to indicate the error information (any critical link event type as shown in Table 7). You can use the log information to track ongoing link status and troubleshoot problems promptly.

Table 7 Critical link events

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>OAMPDU transmission frequencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Fault</td>
<td>Peer link signal is lost.</td>
<td>Once per second.</td>
</tr>
<tr>
<td>Dying Gasp</td>
<td>An unexpected fault, such as power failure, occurred.</td>
<td>Non-stop.</td>
</tr>
</tbody>
</table>

HPE devices can receive and send OAMPDUs carrying the critical link events as follows:

- Receive Information OAMPDUs carrying the critical link events listed in Table 7.
- Do not support sending Information OAMPDUs carrying Link Fault events.
- Do not support sending Information OAMPDUs carrying Dying Gasp events.
- Do not support sending 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 in active 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.

Protocols and standards

IEEE 802.3ah, *Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*
Tasks at a glance

| (Required.) Configuring basic Ethernet OAM functions |
| (Optional.) Configuring the Ethernet OAM connection detection timers |
| (Optional.) Configuring link monitoring |
| • Configuring errored symbol event detection |
| • Configuring errored frame event detection |
| • Configuring errored frame period event detection |
| • Configuring errored frame seconds event detection |
| (Optional.) Configuring the action a port takes after it receives an Ethernet OAM event from the remote end |
| (Optional.) Configuring Ethernet OAM remote loopback |
| • Enabling Ethernet OAM remote loopback for a port in system view |
| • Enabling Ethernet OAM remote loopback for a port in port view |
| • Rejecting the Ethernet OAM remote loopback request from a remote port |

Configuring basic Ethernet OAM functions

To set up an Ethernet OAM connection between two Ethernet OAM entities, you must set at least one entity to operate in active mode. An Ethernet OAM entity can initiate OAM connection only in active mode.

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

To configure basic Ethernet OAM functions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>System-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet port view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Set the Ethernet OAM mode.</td>
<td>oam mode { active</td>
</tr>
<tr>
<td>4.</td>
<td>Enable Ethernet OAM.</td>
<td>oam enable</td>
</tr>
</tbody>
</table>

Configuring the Ethernet OAM connection detection timers

After an Ethernet OAM connection is established, the Ethernet OAM entities exchange Information OAMPDUs at the handshake packet transmission interval to detect the availability of the Ethernet OAM connection. 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.
You can configure this command in system view or port view. The configuration in system view takes effect on all ports, and the configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

After the timeout timer of an Ethernet OAM connection expires, the local OAM entity ages out and terminates its connection with the peer OAM entity. To keep the Ethernet OAM connections stable, set the connection timeout timer to be at least five times the handshake packet transmission interval.

To configure the Ethernet OAM connection detection timers globally:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>System-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the Ethernet OAM handshake packet transmission interval.</td>
<td>oam global timer hello interval</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the Ethernet OAM connection timeout timer.</td>
<td>oam global timer keepalive interval</td>
</tr>
</tbody>
</table>

To configure the Ethernet OAM connection detection timers on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>System-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2/Layer 3 Ethernet port view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the Ethernet OAM handshake packet transmission interval.</td>
<td>oam timer hello interval</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the Ethernet OAM connection timeout timer.</td>
<td>oam timer keepalive interval</td>
</tr>
</tbody>
</table>

### Configuring link monitoring

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

### Configuring errored symbol event detection

An errored symbol event occurs when the number of detected symbol errors in the detection window exceeds the predefined threshold. The detection window refers to the specified number of received symbols.

You can configure this command in system view or port view. The configuration in system view takes effect on all ports, and the configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

To configure errored symbol event detection globally:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the errored symbol event detection window.</td>
<td>oam global errored-symbol-period window window-value</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the errored symbol event triggering threshold.</td>
<td>By default, the errored symbol event triggering threshold is 1.</td>
</tr>
<tr>
<td></td>
<td><code>oam global errored-symbol-period threshold threshold-value</code></td>
<td></td>
</tr>
</tbody>
</table>

To configure errored symbol event detection on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2/Layer 3 Ethernet port view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the errored symbol event detection window.</td>
<td>By default, an interface uses the value configured globally.</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the errored symbol event triggering threshold.</td>
<td>By default, an interface uses the value configured globally.</td>
</tr>
<tr>
<td></td>
<td><code>oam errored-symbol-period window window-value</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>oam errored-symbol-period threshold threshold-value</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring errored frame event detection

An errored frame event occurs when the number of times that error frames in the detection window are detected exceeds the predefined threshold. The detection window refers to the specified detection interval.

You can configure this command in system view or port view. The configuration in system view takes effect on all ports, and the configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

To configure errored frame event detection globally:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the errored frame event detection window.</td>
<td>By default, the errored frame event detection window is 1000 milliseconds.</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the errored frame event triggering threshold.</td>
<td>By default, the errored frame event triggering threshold is 1.</td>
</tr>
<tr>
<td></td>
<td><code>oam global errored-frame window window-value</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>oam global errored-frame threshold threshold-value</code></td>
<td></td>
</tr>
</tbody>
</table>

To configure errored frame event detection on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2/Layer 3 Ethernet port view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the errored frame event detection window.</td>
<td>By default, an interface uses the value configured globally.</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the errored frame event triggering threshold.</td>
<td>By default, an interface uses the value configured globally.</td>
</tr>
<tr>
<td></td>
<td><code>oam errored-frame window window-value</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>oam errored-frame threshold threshold-value</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring errored frame period event detection

An errored frame period event occurs when the number of times that frame errors in the detection window are detected exceeds the predefined threshold. The detection window refers to the specified number of received frames.

You can configure this command in system view or port view. The configuration in system view takes effect on all ports, and the configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

To configure errored frame period event detection globally:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the errored frame period event detection window.</td>
<td>oam global errored-frame-period window window-value</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the errored frame period event triggering threshold.</td>
<td>oam global errored-frame-period threshold threshold-value</td>
</tr>
</tbody>
</table>

To configure errored frame period event detection on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2/Layer 3 Ethernet port view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the errored frame period event detection window.</td>
<td>oam errored-frame-period window window-value</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the errored frame period event triggering threshold.</td>
<td>oam errored-frame-period threshold threshold-value</td>
</tr>
</tbody>
</table>

Configuring errored frame seconds event detection

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

An errored frame seconds event occurs when the number of times that errored frame seconds are detected on a port in the detection window exceeds the predefined threshold. The detection window refers to the specified detection interval.

You can configure this command in system view or port view. The configuration in system view takes effect on all ports, and the configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

To configure errored frame seconds event detection globally:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
To configure errored frame seconds event detection on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Configure the errored frame seconds event detection window.</td>
<td>oam global errored-frame-seconds window window-value</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the errored frame seconds event triggering threshold.</td>
<td>oam global errored-frame-seconds threshold threshold-value</td>
</tr>
</tbody>
</table>

**Configuring the action a port takes after it receives an Ethernet OAM event from the remote end**

This feature enables a port to log events and automatically terminate the OAM connection and set the link state to down.

Follow these restrictions and guidelines when using the dying-gasp and link-fault keywords:
- Only optical ports support the link-fault keyword.
- An optical port that works with the HPE X140 40G QSFP+ LC BiDi 100m MM Transceiver (JL251A) transceiver module does not support the link-fault keyword.

To configure the action the port takes after it receives an Ethernet OAM event from the remote end:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2/Layer 3 Ethernet port view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the action the port takes after it receives an Ethernet OAM event from the remote end.</td>
<td>oam remote-failure { connection-expired</td>
</tr>
</tbody>
</table>
Configuring Ethernet OAM remote loopback

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

After you enable Ethernet OAM remote loopback on a port, the port sends Loopback Control OAMPDUs to a remote port. After receiving the Loopback Control OAMPDUs, 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 and evaluate the link performance.

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

Configuration restrictions and guidelines

- Ethernet OAM remote loopback is available only after the Ethernet OAM connection is established. It 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.
- Enabling Ethernet OAM remote loopback interrupts data communications. After Ethernet OAM remote loopback is disabled, all the ports involved will go down and then come up. Ethernet OAM remote loopback can be disabled by any of the following events:
  - Disabling Ethernet OAM.
  - Disabling Ethernet OAM remote loopback.
  - Timeout of the Ethernet OAM connection.
- Enabling internal loopback test on a port in remote loopback test can terminate the remote loopback test. For more information about loopback test, see Interface Configuration Guide.
- For Ethernet OAM remote loopback to work correctly, do not configure link aggregation management VLANs. For more information about link aggregation management VLANs, see Ethernet link aggregation in Layer 2—LAN Switching Configuration Guide.
- For Ethernet OAM remote loopback to take effect, make sure the peer port is configured with the port bridge enable command (see Ethernet interface commands in Interface Command Reference).

Enabling Ethernet OAM remote loopback for a port in system view

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. (Optional.) Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable Ethernet OAM remote loopback for a port.</td>
<td>oam remote-loopback start interface interface-type interface-number</td>
<td>By default, Ethernet OAM remote loopback is disabled.</td>
</tr>
</tbody>
</table>
Enabling Ethernet OAM remote loopback for a port in port view

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2/Layer 3 Ethernet port view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable Ethernet OAM remote loopback on the port.</td>
<td>oam remote-loopback start</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2/Layer 3 Ethernet port view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Reject the Ethernet OAM remote loopback request from a remote port.</td>
<td>oam remote-loopback reject-request</td>
</tr>
</tbody>
</table>

Displaying and maintaining Ethernet OAM

Execute `display` commands in any view and `reset` commands in user view:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about an Ethernet OAM connection.</td>
<td>`display oam { local</td>
</tr>
<tr>
<td>Display Ethernet OAM configuration.</td>
<td><code>display oam configuration [ interface interface-type interface-number ]</code></td>
</tr>
<tr>
<td>Display the statistics on critical events after an Ethernet OAM connection is established.</td>
<td><code>display oam critical-event [ interface interface-type interface-number ]</code></td>
</tr>
<tr>
<td>Display the statistics on Ethernet OAM link error events after an Ethernet OAM connection is established.</td>
<td>`display oam link-event { local</td>
</tr>
</tbody>
</table>
Task | Command
--- | ---
Clear statistics on Ethernet OAM packets and Ethernet OAM link error events. | reset oam [ interface interface-type interface-number ]

**Ethernet OAM configuration example**

**Network requirements**

On the network shown in Figure 1, perform the following operations:

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

*Figure 1 Network diagram*

**Configuration procedure**

1. **Configure Device A:**
   
   # Configure GigabitEthernet 1/0/1 to operate in active Ethernet OAM mode, and enable Ethernet OAM for it.
   
   `<DeviceA> system-view
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] oam mode active
   [DeviceA-GigabitEthernet1/0/1] oam enable
   
   # Set the errored frame event detection window to 20000 milliseconds, and set the errored frame event triggering threshold to 10.
   [DeviceA-GigabitEthernet1/0/1] oam errored-frame window 200
   [DeviceA-GigabitEthernet1/0/1] oam errored-frame threshold 10
   [DeviceA-GigabitEthernet1/0/1] quit

2. **Configure Device B:**
   
   # Configure GigabitEthernet 1/0/1 to operate in passive Ethernet OAM mode (the default), and enable Ethernet OAM for it.
   
   `<DeviceB> system-view
   [DeviceB] interface gigabitethernet 1/0/1
   [DeviceB-GigabitEthernet1/0/1] oam mode passive
   [DeviceB-GigabitEthernet1/0/1] oam enable
   [DeviceB-GigabitEthernet1/0/1] quit

3. **Verify the configuration:**
   
   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
The output shows that no critical link event occurred on the link between Device A and Device B.

Use the `display oam link-event` command to display the statistics of Ethernet OAM link events. For example:

```
# Display Ethernet OAM link event statistics of the local end of Device A.
[DeviceA] display oam link-event local
```

The output shows the following:

- 350 errors occurred after Ethernet OAM is enabled on Device A.
- 17 errors were caused by error frames.
- The link is unstable.
Configuring CFD

Overview

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 OAM mechanism. CFD is used for link connectivity detection, fault verification, and fault location.

Basic CFD concepts

Maintenance domain

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 introduces eight levels (from 0 to 7) to MDs. The bigger the number, the higher the level and the larger the area covered. Domains can touch or nest (if the outer domain has a higher level than the nested one) but cannot intersect or overlap.

MD levels facilitate fault location and make fault location more accurate. As shown in Figure 2, 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, might fail. If a connectivity fault is also detected at the boundary of MD_B, the failure points can be any of Device B through Device D. If the devices in MD_B can operate correctly, at least Device C is operational.

Figure 2 Two nested MDs

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

Maintenance association

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 the specified VLAN or no VLAN. An MA that serves a VLAN is considered to be carrying VLAN attribute. An MA that serves no VLAN is considered to be carrying no VLAN attribute. 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.
Maintenance point

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

- MEP
  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 equals the level of the MD to which the MEP belongs. 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 packet of its level or lower. The processing procedure is specific to packets in the same VLAN. Packets of different VLANs are independent.
  
  MEPs include inward-facing MEPs and outward-facing MEPs:
  - 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, but it 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 level.
  
  The MA to which a MIP belongs defines the VLAN of packets that the MIP can receive. The level of a MIP is defined by its generation rule and the MD to which the MIP belongs. MIPs are generated on each port automatically according to the following MIP generation rules:
  - Default rule—If no lower-level MIP exists on an interface, a MIP is created on the current level. A MIP can be created even if no MEP is configured on the interface.
  - Explicit rule—If no lower-level MIP exists and a lower-level MEP exists on an interface, a MIP is created on the current level. A MIP can be created only when a lower-level MEP is created on the interface.
  
  If a port has no MIP, the system will check the MAAs in each MD (from low to high levels), and follow the procedure as described in Figure 3 to create or not to create MIPs at the current level.

Figure 3 Procedure of creating MIPs

![Figure 3 Procedure of creating MIPs](image)

Figure 4 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.
- A level 0 outward-facing MEP.

**Figure 4 CFD grading example**

**MEP list**

A MEP list is a collection of local MEPs allowed to be configured and the remote MEPs to be monitored in the same MA. It lists all the 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) carrying a MEP ID not in the MEP list of the MA, it drops the message.

The local device must send CCM messages carrying the Remote Defect Indication (RDI) flag bits. Otherwise, the peer device cannot sense certain failures.

**CFD functions**

CFD 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).

**Continuity check**

Connectivity faults are usually caused by device faults or configuration errors. Continuity check examines the connectivity between MEPs. This function is implemented through periodic sending of CCMs by the MEPs. A CCM sent by one MEP is intended to be received by all 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 as 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.

Loopback

Similar to ping at the IP layer, loopback verifies the connectivity between a source device and a
target device. To implement this function, the source MEP sends loopback messages (LBM) 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 are multicast and unicast frames. HPE devices support sending and receiving unicast
LBM frames and receiving multicast LBM frames. HPE devices do not support sending multicast
LBM frames. LBR frames are unicast frames.

Linktrace

Linktrace is similar to traceroute. It identifies the path between the source MEP and the target MP.
The source MEP sends the linktrace messages (LTM) to the target MP. After receiving the
messages, the target MP and the MIPs that the LTM frames pass send back linktrace reply
messages (LTR) 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 does not
receive any CCM frames from its peer MEP within 3.5 times the CCM transmission interval, it
immediately starts sending AIS frames. The AIS frames are sent periodically in the opposite direction
of CCM frames. When the peer MEP receives the AIS frames, it 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 (LMM) to the target MEP. The target MEP responds with
loss measurement replies (LMR). 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 unicast frames.

DM

The DM function measures frame delays between two MEPs, including the following types:

- 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. When the target MEP receives the 1DM frame, it does the
  following:
  - Records the reception time.
  - Calculates and records the link transmission delay and jitter (delay variation) according to
    the transmission time and reception time.

  1DM frames are unicast frames.

- Two-way frame delay measurement
  The source MEP sends a delay measurement message (DMM), which carries the transmission
  time, to the target MEP. When the target MEP receives the DMM, it responds with a delay
  measurement reply (DMR). The DMR carries the reception time and transmission time of the
  DMM and the transmission time of the DMR. When the source MEP receives the DMR, it does
  the following:
  - Records the DMR reception time.
Calculates the link transmission delay and jitter according to the DMR reception time and DMM transmission time. DMM frames and DMR frames are unicast 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. When the target MEP receives the TST frame, it determines the bit errors by calculating and comparing the content of the TST frame. TST frames are unicast frames.

**EAIS**

Ethernet Alarm Indication Signal (EAIS) enables collaboration between the Ethernet port status and the AIS function. When a port on the device (not necessarily an MP) goes down, it immediately starts to send EAIS frames periodically to suppress the error alarms. When the port goes up again, it immediately stops sending EAIS frames. When the MEP receives the EAIS frames, it suppresses the error alarms locally, and continues to send the EAIS frames. If a MEP receives no EAIS frames within 3.5 times the EAIS frame transmission interval, the fault is considered cleared. The port stops sending EAIS frames and restores the error alarm function. EAIS frames are multicast 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*

**Configuration restrictions and guidelines**

CFD is not supported by OAP modules. For more information about OAP modules, see *OAA Configuration Guide*.

**CFD configuration task list**

For CFD to work correctly, 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 that the devices in the same MD use the same MD name.
- Define the MA in each MD according to the VLAN you want to monitor.
- Assign a name for each MA. Make sure that the devices in the same MA in the same MD use the same MA name.
- Determine the MEP list of each MA in each MD. Make sure that devices in the same MA maintain the same MEP list.
- At the edges of MD and MA, MEPs must be designed at the device port. MIPs can be designed on devices or ports that are not at the edges.

To configure CFD, perform the following tasks:

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring basic CFD settings:</td>
</tr>
<tr>
<td>• (Required.) Enabling CFD</td>
</tr>
</tbody>
</table>
### Tasks at a glance
- (Required.) Configuring Ethernet service instances
- (Required.) Configuring MEPs
- (Required.) Configuring MIP auto-generation rules

### Configuring CFD functions:
- (Required.) Configuring CC
- (Optional.) Configuring LB
- (Optional.) Configuring LT
- (Optional.) Configuring AIS
- (Optional.) Configuring LM
- (Optional.) Configuring one-way DM
- (Optional.) Configuring two-way DM
- (Optional.) Configuring TST
- (Optional.) Configuring EAIS

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 inward-facing MEP, which 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

#### Enabling CFD

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable CFD.</td>
<td>cfd enable</td>
</tr>
</tbody>
</table>

#### Configuring Ethernet service instances

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

The MD and MA define the level attribute and VLAN attribute of the messages handled by the MPs in an Ethernet service instance. The MPs of the MA that carries no VLAN attribute do not belong to any VLAN.

To configure an Ethernet service instance with the MD name:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an MD.</td>
<td>cfd md md-name [ index index-value ] level level-value</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>3.</td>
<td>Create an Ethernet service instance.</td>
<td>By default, no Ethernet service instance exists.</td>
</tr>
</tbody>
</table>

### Configuring MEPS

CFD is implemented through various operations on MEPS. As a MEP is configured on an Ethernet service instance, the MD level and VLAN attribute of the Ethernet service instance become the attribute of the MEP.

Before creating MEPS, configure the MEP list. A MEP list is a collection of local MEPS that can be configured in an MA and the remote MEPS to be monitored. You cannot create a MEP if the MEP ID is not included in the MEP list of the Ethernet service instance.

You can specify an interface as the MEP for only one of the non-VLAN-specific MAs at the same level. In addition, the MEP must be outward facing.

CFD sets the link state for an interface to down if the following conditions exist:

- The MEP configured on the interface is in an MA carrying no VLAN attribute.
- The MEP does not receive any CCM messages from its peer MEP within 3.5 times the CCM transmission interval.

To configure a MEP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure a MEP list.</td>
<td>cfd meplist mep-list service-instance instance-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type service-instance instance-id interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Create a MEP.</td>
<td>cfd mep mep-id service-instance instance-id { inbound</td>
</tr>
</tbody>
</table>

### Configuring MIP auto-generation rules

As functional entities in an Ethernet service instance, MIPs respond to various CFD frames, such as LTM and LBM frames. You can configure MIP auto-generation rules for the system to automatically create MIPs.

Any of the following events can cause MIPs to be created or deleted after you have configured the cfd mip-rule command:

- Enabling or disabling CFD.
- Creating or deleting MEPS on a port.
- Changes occur to the VLAN attribute of a port.
- The rule specified in the cfd mip-rule command changes.

An MA carrying no VLAN attribute is typically used to detect direct link status. The system cannot generate MIPs for such MAs.
For an MA carrying VLAN attribute, the system does not generate MIPs if the same or a higher level MEP exists on the interface.

To configure the rules for generating MIPs:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure MIP auto-generation</td>
<td>cfd mip-rule { default</td>
</tr>
</tbody>
</table>

By default, no rules for generating MIPs are configured, and the system does not automatically create any MIP.

**Configuring CFD functions**

**Configuration prerequisites**

Complete basic CFD settings.

**Configuring CC**

Configure CC before you use the MEP ID of the remote MEP to configure other CFD functions. This restriction does not apply when you use the MAC address of the remote MEP to configure other CFD functions.

After the CC function is configured, MEPs in an MA can periodically send CCM frames to maintain connectivity. When the lifetime of a CCM frame expires, the link to the sending MEP is considered disconnected. When setting the CCM interval, use the settings described in Table 8.

**Table 8 CCM interval field encoding**

<table>
<thead>
<tr>
<th>CCM interval field</th>
<th>Transmission interval</th>
<th>Maximum CCM lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>100 milliseconds</td>
<td>350 milliseconds</td>
</tr>
<tr>
<td>4</td>
<td>1 second</td>
<td>3.5 seconds</td>
</tr>
<tr>
<td>5</td>
<td>10 seconds</td>
<td>35 seconds</td>
</tr>
<tr>
<td>6</td>
<td>60 seconds</td>
<td>210 seconds</td>
</tr>
<tr>
<td>7</td>
<td>600 seconds</td>
<td>2100 seconds</td>
</tr>
</tbody>
</table>

**NOTE:**

- The value range for the interval field value is 3 to 7.
- The CCM messages with an interval field value of 1 to 3 are short-interval CCM messages. The CCM messages with an interval field value of 4 to 7 are long-interval CCM messages.

Follow these guidelines when you configure CC on a MEP:

- Configure the same CCM interval field value for all MEPs in the same MA.
- After the CCM interval field is modified, the MEP must wait for another CCM interval before sending CCMs.
- Setting the CCM interval field value to smaller than 4 might cause the CC function to operate unsteadily.
- If the device has multiple cards with auxiliary CPUs, all MEPs on the device send CCM frames through one of these cards. If the sending card is removed, another card takes over to send
CCM frames. If all these cards are removed, MEPs with a short CCM interval immediately stop sending CCM frames. MEPs with a long CCM interval send CCM frames through the cards where the MEPs are created.

- The cards without auxiliary CPUs discard short-interval CCM messages to reduce impact on CPU performance. If your device does not have an auxiliary CPU, configure a long CCM interval for all MEPs.

To configure CC on a MEP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Set the CCM interval field.</td>
<td>cfd cc interval interval-value service-instance instance-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Enable CCM sending on a MEP.</td>
<td>cfd cc service-instance instance-id mep mep-id enable</td>
</tr>
</tbody>
</table>

### Configuring LB

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

To configure LB on a MEP:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable LB.</td>
<td>cfd loopback service-instance instance-id mep mep-id { target-mac mac-address</td>
<td>target-mep target-mep-id } [ number number ]</td>
</tr>
</tbody>
</table>

### Configuring LT

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

- **Tracing path**—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 is identified.

- **LT messages automatic sending**—If the source MEP fails to receive CCM frames from the target MEP within 3.5 times the transmission interval, it considers the link faulty. The source MEP then sends LTM frames, with the TTL field set to the maximum value 255, to the target MEP. Based on the returned LTRs, the fault source is located.

**IMPORTANT:**

Before you configure LT on a MEP in an MA carrying VLAN attribute, create the VLAN to which the MA belongs.

To configure LT on MEPs:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Identify the path between a source MEP and a target MEP.</td>
<td>cfd linktrace service-instance instance-id mep mep-id { target-mac mac-address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>target-mep target-mep-id } [ ttl ttl-value ] [ hw-only ]</td>
</tr>
<tr>
<td>2.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>3.</td>
<td>Enable LT messages automatic sending.</td>
<td>cfd linktrace auto-detection [ size size-value ]</td>
</tr>
</tbody>
</table>

### Configuring AIS

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

To make a MEP in the Ethernet service instance send AIS frames, set the AIS frame transmission level to be higher than the MD level of the MEP.

Enable AIS and configure a correct AIS frame transmission level on the target MEP, so the target MEP can do the following:

- Suppress the error alarms.
- Send the AIS frame to the MD of a higher level.

If you enable AIS but do not configure a correct AIS frame transmission level, the target MEP can suppress the error alarms, but cannot send the AIS frames.

To configure AIS:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable AIS.</td>
<td>cfd ais enable</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the AIS frame transmission level.</td>
<td>cfd ais level level-value service-instance instance-id</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the AIS frame transmission interval.</td>
<td>cfd ais period period-value service-instance instance-id</td>
</tr>
</tbody>
</table>

### Configuring LM

The LM function measures frame loss between MEPs. Frame loss statistics include the number of lost frames, the frame loss ratio, and the average number of lost frames for the source and target MEPs.

To configure LM:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure LM.</td>
<td>cfd slm service-instance instance-id mep mep-id { target-mac mac-address</td>
<td>Available in any view.</td>
</tr>
<tr>
<td></td>
<td>target-mep target-mep-id } [ dot1p dot1p-value ] [ number number ] [ interval interval ]</td>
<td></td>
</tr>
</tbody>
</table>
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.

One-way DM requires that the time setting at the transmitting MEP and the receiving MEP be the same. For the purpose of frame delay variation measurement, the requirement can be relaxed.

To view the test result, use the `display cfd dm one-way history` command on the target MEP.

To configure one-way DM:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure one-way DM.</td>
<td>`cfd dm one-way service-instance instance-id mep mep-id { target-mac mac-address</td>
<td>target-mep target-mep-id } [ number number]`</td>
</tr>
</tbody>
</table>

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. It also monitors and manages the link transmission performance.

To configure two-way DM:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure two-way DM.</td>
<td>`cfd dm two-way service-instance instance-id mep mep-id { target-mac mac-address</td>
<td>target-mep target-mep-id } dot1p dot1p-value ] [ number number] [ interval interval ]`</td>
</tr>
</tbody>
</table>

Configuring TST

The TST function detects bit errors on a link, and monitors and manages the link transmission performance.

To view the test result, use the `display cfd tst` command on the target MEP.

To configure TST:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure TST.</td>
<td>`cfd tst service-instance instance-id mep mep-id { target-mac mac-address</td>
<td>target-mep target-mep-id } [ number number] [ length-of-test length ] [ pattern-of-test { all-zero</td>
</tr>
</tbody>
</table>
Configuring EAIS

You can configure EAIS on a device that does not support or is not configured with CFD. However, EAIS must collaborate with the CFD function in the network, so you must configure CFD in the network.

To make a port send the EAIS frames, configure port status-AIS collaboration, and configure the correct EAIS frame transmission level and interval. If you only enable port status-EAIS collaboration, but do not configure the EAIS frame transmission level and interval, the port cannot send EAIS frames.

If you do not specify the VLANs where the EAIS frames can be transmitted, the EAIS frames will be transmitted in the default VLAN of the current port. Otherwise, the EAIS frames will be transmitted in the intersection of the following VLANs:

- Specified VLANs where the EAIS frames can be transmitted.
- VLANs to which the port belongs.

If you configure EAIS on the member port of an aggregation group, the EAIS configuration does not take effect until the port leaves the aggregation group.

If the intersection of the configured VLANs where the EAIS frames can be transmitted and the VLANs to which the port belongs is empty, no EAIS frame is sent. If the intersection contains more than 70 VLANs and the EAIS frame transmission interval is 1 second, the CPU usage will be too high. As a best practice, set the EAIS frame transmission interval to 60 seconds in this case.

To configure EAIS:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable port status-AIS collaboration.</td>
<td>cfd ais-track link-status global</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the EAIS frame transmission level.</td>
<td>cfd ais-track link-status level level-value</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the EAIS frame transmission interval.</td>
<td>cfd ais-track link-status period period-value</td>
</tr>
<tr>
<td>6.</td>
<td>Specify the VLANs where the EAIS frames can be transmitted.</td>
<td>cfd ais-track link-status vlan vlan-list</td>
</tr>
</tbody>
</table>

Displaying and maintaining CFD

Execute **display** commands in any view and **reset** commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the AIS configuration and information on the specified MEP.</td>
<td>display cfd ais [ service-instance instance-id [ mep mep-id ] ]</td>
</tr>
<tr>
<td>Display the AIS configuration and information associated with the status of the specified port.</td>
<td>display cfd ais-track link-status [ interface interface-type interface-number ]</td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display the one-way DM result on the specified MEP.</td>
<td>display cfd dm one-way history [ service-instance instance-id [ mep mep-id ] ]</td>
</tr>
<tr>
<td>Display LTR information received by a MEP.</td>
<td>display cfd linktrace-reply [ service-instance instance-id [ mep mep-id ] ]</td>
</tr>
<tr>
<td>Display the content of the LTR messages received as responses to the automatically sent LTMs.</td>
<td>display cfd linktrace-reply auto-detection [ size size-value ]</td>
</tr>
<tr>
<td>Display MD configuration information.</td>
<td>display cfd md</td>
</tr>
<tr>
<td>Display the attribute and running information of the MEPs.</td>
<td>display cfd mep mep-id service-instance instance-id</td>
</tr>
<tr>
<td>Display MEP list in an Ethernet service instance.</td>
<td>display cfd meplist [ service-instance instance-id ]</td>
</tr>
<tr>
<td>Display MP information.</td>
<td>display cfd mp [ interface interface-type interface-number ]</td>
</tr>
<tr>
<td>Display information about a remote MEP.</td>
<td>display cfd remote-mep service-instance instance-id mep mep-id</td>
</tr>
<tr>
<td>Display Ethernet service instance configuration information.</td>
<td>display cfd service-instance [ instance-id ]</td>
</tr>
<tr>
<td>Display CFD status.</td>
<td>display cfd status</td>
</tr>
<tr>
<td>Display the TST result on the specified MEP.</td>
<td>display cfd tst [ service-instance instance-id [ mep mep-id ] ]</td>
</tr>
<tr>
<td>Clear the one-way DM result on the specified MEP.</td>
<td>reset cfd dm one-way history [ service-instance instance-id [ mep mep-id ] ]</td>
</tr>
<tr>
<td>Clear the TST result on the specified MEP.</td>
<td>reset cfd tst [ service-instance instance-id [ mep mep-id ] ]</td>
</tr>
</tbody>
</table>

CFD configuration example

Network requirements

As shown in Figure 5:

- 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-FC01-6511, 0010-FC02-6512, 0010-FC03-6513, 0010-FC04-6514, and 0010-FC05-6515, 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. You must 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 must 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 and EAIS functions to suppress the error alarms that are 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.
Configuration procedure

1. Configure a VLAN and assign ports to it:
   On each device shown in Figure 5, 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
   # Configure Device B through Device E in the same way Device A is configured. (Details not shown.)

3. Configure Ethernet service instances:
   # Create MD_A (level 5) on Device A, and create Ethernet service instance 1 (in which the MA is identified by a VLAN and serves VLAN 100).
   [DeviceA] cfd md MD_A level 5
   [DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 100
   # Configure Device E in the same way Device A is configured. (Details not shown.)
   # Create MD_A (level 5) on Device B, and create Ethernet service instance 1 (in which the MA is identified by a VLAN and serves VLAN 100).
   [DeviceB] cfd md MD_A level 5
   [DeviceB] cfd service-instance 1 ma-id vlan-based md MD_A vlan 100
   # Create MD_B (level 3), and create Ethernet service instance 2 (in which the MA is identified by a VLAN and serves VLAN 100).
   [DeviceB] cfd md MD_B level 3
   [DeviceB] cfd service-instance 2 ma-id vlan-based md MD_B vlan 100
   # Configure Device D in the same way Device B is configured. (Details not shown.)
   # Create MD_B (level 3) on Device C, and create Ethernet service instance 2 (in which the MA is identified by a VLAN and serves VLAN 100).
   [DeviceC] cfd md MD_B level 3
   [DeviceC] cfd service-instance 2 ma-id vlan-based md MD_B vlan 100

4. Configure MEPs:
# On Device A, configure a MEP list in Ethernet service instance 1, and create inward-facing MEP 1001 in Ethernet 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] quit

# On Device B, configure a MEP list in Ethernet service instances 1 and 2.

[DeviceB] cfd meplist 1001 4002 5001 service-instance 1
[DeviceB] cfd meplist 2001 4001 service-instance 2

# Create outward-facing MEP 2001 in Ethernet service instance 2 on GigabitEthernet 1/0/3.

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

# On Device D, configure a MEP list in Ethernet service instances 1 and 2.

[DeviceD] cfd meplist 1001 4002 5001 service-instance 1
[DeviceD] cfd meplist 2001 4001 service-instance 2

# Create outward-facing MEP 4001 in Ethernet service instance 2 on GigabitEthernet 1/0/1.

[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd mep 4001 service-instance 2 outbound
[DeviceD-GigabitEthernet1/0/1] quit

# Create inward-facing MEP 4002 in Ethernet service instance 1 on GigabitEthernet 1/0/3.

[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] cfd mep 4002 service-instance 1 inbound
[DeviceD-GigabitEthernet1/0/3] quit

# On Device E, configure a MEP list in Ethernet service instance 1.

[DeviceE] cfd meplist 1001 4002 5001 service-instance 1

# Create inward-facing MEP 5001 in Ethernet service instance 1 on GigabitEthernet 1/0/4.

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

5. Configure MIPs:

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

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

# Configure the MIP generation rule in Ethernet 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 Ethernet 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 Ethernet 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 Ethernet service instance 2 on GigabitEthernet 1/0/1.

[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 2 mep 4001 enable
[DeviceD-GigabitEthernet1/0/1] quit
7. Configure AIS:

# Enable AIS on Device B. Configure the AIS frame transmission level as 5 and AIS frame transmission interval as 1 second in Ethernet service instance 2.

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

8. Configure EAIS:

# Enable port status-AIS collaboration on Device B.

[DeviceB] cfd ais-track link-status global

# On GigabitEthernet 1/0/3 of Device B, configure the EAIS frame transmission level as 5 and the EAIS frame transmission interval as 60 seconds. Specify the VLANs where the EAIS frames can be transmitted as VLAN 100.

[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] cfd ais-track link-status level 5
[DeviceB-GigabitEthernet1/0/3] cfd ais-track link-status period 60
[DeviceB-GigabitEthernet1/0/3] cfd ais-track link-status vlan 100
[DeviceB-GigabitEthernet1/0/3] quit

Verifying the configuration

1. Verify the LB function when the CC function detects a link fault:

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

[DeviceA] cfd loopback service-instance 1 mep 1001 target-mep 5001
Loopback to MEP 5001 with the sequence number start from 1001-43404:
Reply from 0010-fc05-6515: sequence number=1001-43404 time=5ms
Reply from 0010-fc05-6515: sequence number=1001-43405 time=5ms
Reply from 0010-fc05-6515: sequence number=1001-43406 time=5ms
Reply from 0010-fc05-6515: sequence number=1001-43407 time=5ms
Reply from 0010-fc05-6515: sequence number=1001-43408 time=5ms
Sent: 5    Received: 5    Lost: 0

2. Verify the LT function after the CC function obtains the status information of the entire network:

# Identify the path between MEP 1001 and MEP 5001 in Ethernet 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
3. Verify the LM function after the CC function obtains the status information of the entire network:

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

[DeviceA] cfd slm service-instance 1 mep 1001 target-mep 4002

Reply from 0010-fc04-6514
Far-end frame loss: 10   Near-end frame loss: 20
Reply from 0010-fc04-6514
Far-end frame loss: 40   Near-end frame loss: 40
Reply from 0010-fc04-6514
Far-end frame loss: 0    Near-end frame loss: 10
Reply from 0010-fc04-6514
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: 25.00%  Near-end frame loss rate: 32.00%
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:

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

[DeviceA] cfd dm one-way service-instance 1 mep 1001 target-mep 4002
5 1DMs have been sent. Please check the result on the remote device.

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

[DeviceD] display cfd dm one-way history service-instance 1 mep 4002
Service instance: 1
MEP ID: 4002
Sent 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:

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

[DeviceA] cfd dm two-way service-instance 1 mep 1001 target-mep 4002
Frame delay:
Reply from 0010-fc04-6514: 2406us
Reply from 0010-fc04-6514: 2215us
Reply from 0010-fc04-6514: 2112us
Reply from 0010-fc04-6514: 1812us
Reply from 0010-fc04-6514: 2249us
Average: 2158us
Sent DMMs: 5   Received: 5   Lost: 0

Frame delay variation: 191us 103us 300us 437us
6. **Verify the TST function after the CC function obtains the status information of the entire network:**

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

   [DeviceA] cfd tst service-instance 1 mep 1001 target-mep 4002
   5 TSTs have been sent. Please check the result on the remote device.

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

   [DeviceD] display cfd tst service-instance 1 mep 4002
   Service instance: 1
   MEP ID: 4002
   Sent TST total number: 0
   Received TST total number: 5
   Received from 0010-fc01-6511, Bit True, sequence number 0
   Received from 0010-fc01-6511, Bit True, sequence number 1
   Received from 0010-fc01-6511, Bit True, sequence number 2
   Received from 0010-fc01-6511, Bit True, sequence number 3
   Received from 0010-fc01-6511, Bit True, sequence number 4
Configuring DLDP

Overview

A link becomes unidirectional when only one end of the link can receive packets from the other end. Unidirectional fiber links occur in the following cases:

- Fibers are cross-connected.
- A fiber is not connected at one end or one fiber of a fiber pair is broken.

Figure 6 shows a correct fiber connection and two types of unidirectional fiber connections.

**Figure 6 Correct and incorrect fiber connections**

Physical layer detection mechanisms, such as auto-negotiation, can detect physical signals and faults. However, they cannot detect communication failures for unidirectional links where the physical layer is in connected state.

As a data link layer protocol, the Device Link Detection Protocol (DLDP) detects the following:

- Whether the fiber link or twisted-pair link is correctly connected at the link layer.
- Whether the two ends of the link can exchange packets correctly.

When DLDP detects unidirectional links, it can automatically shut down the faulty port to avoid network problems. Alternatively, a user can manually shut down the faulty port. DLDP cooperates with physical layer protocols to monitor link status and avoid physical and logical unidirectional links.
Basic concepts

DLDP neighbor states
If port A can receive link-layer packets from port B on the same link, port B is a DLDP neighbor of port A. Two ports that can exchange packets are neighbors.

<table>
<thead>
<tr>
<th>DLDP timer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirmed</td>
<td>The link to a DLDP neighbor is bidirectional.</td>
</tr>
<tr>
<td>Unconfirmed</td>
<td>The state of the link to a newly discovered neighbor is not determined.</td>
</tr>
</tbody>
</table>

DLDP port states
A DLDP-enabled port is called a DLDP port. A DLDP port can have multiple neighbors, and its state varies by the DLDP neighbor state.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>DLDP is enabled on the port, but is disabled globally.</td>
</tr>
<tr>
<td>Inactive</td>
<td>DLDP is enabled on the port and globally, and the link is physically down.</td>
</tr>
<tr>
<td>Bidirectional</td>
<td>DLDP is enabled on the port and globally, and at least one neighbor in Confirmed state exists.</td>
</tr>
<tr>
<td>Unidirectional</td>
<td>DLDP is enabled on the port and globally, and no neighbor in Confirmed state exists. In this state, a port does not send or receive packets other than DLDP packets any more.</td>
</tr>
</tbody>
</table>

DLDP timers

<table>
<thead>
<tr>
<th>DLDP timer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertisement timer</td>
<td>Advertisement packet sending interval (the default is 5 seconds and is configurable).</td>
</tr>
<tr>
<td>Probe timer</td>
<td>Probe packet sending interval. This timer is set to 1 second.</td>
</tr>
<tr>
<td>Echo timer</td>
<td>The Echo timer is triggered when a probe is launched for a new neighbor. This timer is set to 10 seconds.</td>
</tr>
<tr>
<td>Entry timer</td>
<td>When a new neighbor joins, a neighbor entry is created and the corresponding entry timer is triggered if the neighbor is in Confirmed state. When an Advertisement is received, the device updates the corresponding neighbor entry and the Entry timer. The setting of an Entry timer is three times that of the Advertisement timer.</td>
</tr>
<tr>
<td>Enhanced timer</td>
<td>The Enhanced timer is triggered, together with the Echo timer, when the Entry timer expires. The Enhanced timer is set to 1 second.</td>
</tr>
<tr>
<td>DelayDown timer</td>
<td>If a port is physically down, the device triggers the DelayDown timer, rather than removing the corresponding neighbor entry. The default DelayDown timer is 1 second and is configurable. When the DelayDown timer expires, the device removes the corresponding DLDP neighbor information if the port is down, and does not perform any operation if the port is up.</td>
</tr>
<tr>
<td>DLDP timer</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RecoverProbe timer</td>
<td>This timer is set to 2 seconds. A port in Unidirectional state regularly sends RecoverProbe packets to detect whether a unidirectional link has been restored to bidirectional.</td>
</tr>
</tbody>
</table>

**DLDP authentication mode**

You can use DLDP authentication to prevent network attacks and illegal detecting.

**Table 12 DLDP authentication mode**

<table>
<thead>
<tr>
<th>Authentication mode</th>
<th>Processing at the DLDP packet sending side</th>
<th>Processing at the DLDP packet receiving side</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-authentication</td>
<td>The sending side sets the Authentication field of DLDP packets to 0.</td>
<td>The receiving side examines the authentication information of received DLDP packets and drops packets where the authentication information conflicts with the local configuration.</td>
</tr>
<tr>
<td>Plaintext authentication</td>
<td>The sending side sets the Authentication field to the password configured in plain text.</td>
<td></td>
</tr>
<tr>
<td>MD5 authentication</td>
<td>The sending side encrypts the user configured password by using MD5 algorithm, and assigns the digest to the Authentication field.</td>
<td></td>
</tr>
</tbody>
</table>

**How DLDP works**

**Detecting one neighbor**

When two devices are connected through an optical fiber or a network cable, enable DLDP to detect unidirectional links to the neighbor. The following illustrates the unidirectional link detection process in two cases:

- Unidirectional links occur before you enable DLDP.

*Figure 7 Cross-connected fibers*

As shown in *Figure 7*, before you enable DLDP, the optical fibers between Device A and Device B are cross-connected. After you enable DLDP, the four ports are all up and in Unidirectional state, and they send RecoverProbe packets. Take Port 1 as an example to illustrate the unidirectional link detection process.

a. Port 1 receives the RecoverProbe packet from Port 4, and returns a RecoverEcho packet.

b. Port 4 cannot receive any RecoverEcho packet from Port 1, so Port 4 cannot become the neighbor of Port 1.

c. Port 3 can receive the RecoverEcho packet from Port 1, but Port 3 is not the intended destination, so Port 3 cannot become the neighbor of Port 1.

The same process occurs on the other three ports. The four ports are all in Unidirectional state.

- Unidirectional links occur after you enable DLDP.
As shown in Figure 8, Device A and Device B are connected through an optical fiber. After you enable DLDP, Port 1 and Port 2 establish the bidirectional neighborhood in the following way:

- **a.** Port 1 that is physically up enters the Unidirectional state and sends a RecoverProbe packet.
- **b.** After receiving the RecoverProbe packet, Port 2 returns a RecoverEcho packet.
- **c.** After Port 1 receives the RecoverEcho packet, it examines the neighbor information in the packet. If the neighbor information matches the local information, Port 1 establishes the neighborhood with Port 2 and transits to Bidirectional state. Port 1 then starts the Entry timer and periodically sends Advertisement packets.
- **d.** After Port 2 receives the Advertisement packet, it establishes the Unconfirmed neighborhood with Port 1. Port 2 then starts the Echo timer and Probe timer, and periodically sends Probe packets.
- **e.** After receiving the Probe packet, Port 1 returns an Echo packet.
- **f.** After Port 2 receives the Echo packet, it examines the neighbor information in the packet. If the neighbor information matches the local information, the neighbor state of Port 1 becomes Confirmed. Port 2 then transits to Bidirectional state, starts the Entry timer, and periodically sends Advertisement packets.

The bidirectional neighborhood between Port 1 and Port 2 is now established.

After that, when Port 2's Rx end fails to receive signals, Port 2 is physically down and enters the Inactive state. Because Port 2's Tx end can still send signals to Port 1, Port 1 stays up. After the Entry timer for Port 2 expires, Port 1 starts the Enhanced timer and Echo timer, and sends a probe packet to Port 2. Because Port 1's Tx line is broken, Port 1 cannot receive the Echo packet from Port 2 after the Echo timer expires. Port 1 then enters the Unidirectional state, and sends a Disable packet to Port 2. At the same time, Port 1 deletes the neighborhood with Port 2, and starts the RecoverProbe timer. Port 2 stays in Inactive state during this process.

DLDP sends a LinkDown packet to inform the peer to delete the relevant neighbor entry for an interface when the following conditions exist:

- The interface is a GE fiber interface that operates at 1000 Mbps in full duplex mode.
  
  For how to configure the speed and duplex mode for an interface, see *Interface Command Reference*.
- The Rx end goes down but the Tx end is up for the interface.
Detecting multiple neighbors

When multiple devices are connected through a hub, enable DLDP on all interfaces connected to the hub to detect unidirectional links among the neighbors. When no Confirmed neighbor exists, an interface enters the Unidirectional state.

Figure 9 Network diagram

As shown in Figure 9, Device A through Device D are connected through a hub, and enabled with DLDP. When Ports 1, 2, and 3 detect that the link to Port 4 fails, they delete the neighborship with Port 4, but stay in Bidirectional state.

Configuration restrictions and guidelines

When you configure DLDP, follow these configuration restrictions and guidelines:

- For DLDP to operate correctly, enable DLDP on both sides and make sure the following settings are consistent:
  - Interval to send Advertisement packets.
  - DLDP authentication mode.
  - Password.
- For DLDP to operate correctly, configure the full duplex mode for the ports at the two ends of the link, and configure the same speed for the two ports.

DLDP configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Enabling DLDP</td>
</tr>
<tr>
<td>(Optional.) Setting the interval to send advertisement packets</td>
</tr>
<tr>
<td>(Optional.) Setting the DelayDown timer</td>
</tr>
<tr>
<td>(Optional.) Setting the port shutdown mode</td>
</tr>
<tr>
<td>(Optional.) Configuring DLDP authentication</td>
</tr>
</tbody>
</table>
Enabling DLDP

To correctly configure DLDP on the device, you must enable DLDP globally and on each port.

To enable DLDP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable DLDP globally.</td>
<td>dldp global enable</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Enable DLDP.</td>
<td>dldp enable</td>
</tr>
</tbody>
</table>

Setting the interval to send advertisement packets

To make sure DLDP can detect unidirectional links before network performance deteriorates, set the advertisement interval appropriate for your network environment. (As a best practice, use the default interval.)

To set the Advertisement packet sending interval:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Set the interval to send Advertisement packets.</td>
<td>dldp interval interval</td>
<td>By default, the interval is 5 seconds.</td>
</tr>
</tbody>
</table>

Setting the DelayDown timer

When the Tx line fails, some ports might go down and then come up again, causing optical signal jitters on the Rx line. To prevent the device from removing neighbor entries in such cases, set the DelayDown timer for the device. The device starts the DelayDown timer when a port goes down due to a Tx line failure. If the port remains down when the timer expires, the device removes the DLDP neighbor information. If the port comes up, the device takes no action.

To set the DelayDown timer:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Set the DelayDown timer.</td>
<td>dldp delaydown-timer time</td>
<td>The default is 1 second. The DelayDown timer setting applies to all DLDP-enabled ports.</td>
</tr>
</tbody>
</table>

Setting the port shutdown mode

On detecting a unidirectional link, DLDP shuts down the ports in one of the following modes:
• **Auto mode**—When DLDP detects a unidirectional link, it shuts down the Unidirectional port. When the link becomes Bidirectional, DLDP brings up the port that was shut down.

• **Hybrid mode**—When DLDP detects a unidirectional link, it shuts down the Unidirectional port and stops link detection. To verify the link status, use the `undo shutdown` command to bring up the port. If the link becomes Bidirectional, the port becomes Bidirectional.

• **Manual mode**—When DLDP detects a unidirectional link, it does not shut down the port. You need to manually shut it down. When the link becomes Bidirectional, you must manually bring up the port. Use this mode to prevent normal links from being shut down because of false unidirectional link reports in the following cases:
  - The network performance is low.
  - The device is busy.
  - The CPU usage is high.

To enable remote OAM loopback on a DLDP port, set the port shutdown mode to `manual`. Otherwise, DLDP automatically shuts down the port when it receives a packet sent by itself. This causes remote OAM loopback failure. For more information about Ethernet OAM, see "Configuring Ethernet OAM."

To set port shutdown mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Set port shutdown mode.</td>
<td>`dldp unidirectional-shutdown { auto</td>
</tr>
</tbody>
</table>

### Configuring DLDP authentication

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

To configure DLDP authentication:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Configure a DLDP authentication mode.</td>
<td>`dldp authentication-mode { md5</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the password for DLDP authentication.</td>
<td>`dldp authentication-password { cipher</td>
</tr>
</tbody>
</table>

### Displaying and maintaining DLDP

Execute `display` commands in any view and the `reset` command in user view.
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the DLDP configuration globally and of a port.</td>
<td><code>display dldp</code></td>
</tr>
<tr>
<td>Display the statistics on DLDP packets passing through a port.</td>
<td><code>display dldp statistics</code></td>
</tr>
<tr>
<td>Clear the statistics on DLDP packets passing through a port.</td>
<td><code>reset dldp statistics</code></td>
</tr>
</tbody>
</table>

### DLDP configuration examples

#### Configuring the auto port shutdown mode

**Network requirements**

As shown in Figure 10, Device A and Device B are connected through 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 10 Network diagram**

![Network diagram](image)

**Configuration procedure**

1. Configure Device A:

   ```
   # Enable DLDP globally.
   <DeviceA> system-view
   [DeviceA] dldp global enable
   # Configure GigabitEthernet 1/0/1 to operate in full duplex mode and at 1000 Mbps, and enable DLDP on the port.
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] duplex full
   [DeviceA-GigabitEthernet1/0/1] speed 1000
   [DeviceA-GigabitEthernet1/0/1] dldp enable
   [DeviceA-GigabitEthernet1/0/1] quit
   # Configure GigabitEthernet 1/0/2 to operate in full duplex mode and at 1000 Mbps, and enable DLDP on the port.
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] duplex full
   [DeviceA-GigabitEthernet1/0/2] speed 1000
   [DeviceA-GigabitEthernet1/0/2] dldp enable
   [DeviceA-GigabitEthernet1/0/2] quit
   # Set the port shutdown mode to auto.
   ```
Configure Device B:

# Enable DLDP globally.
<DeviceB> system-view
[DeviceB] dldp global enable

# Configure GigabitEthernet 1/0/1 to operate in full duplex mode and at 1000 Mbps, and enable DLDP on it.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] duplex full
[DeviceB-GigabitEthernet1/0/1] speed 1000
[DeviceB-GigabitEthernet1/0/1] dldp enable
[DeviceB-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 to operate in full duplex mode and at 1000 Mbps, and enable DLDP on it.
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] duplex full
[DeviceB-GigabitEthernet1/0/2] speed 1000
[DeviceB-GigabitEthernet1/0/2] dldp enable
[DeviceB-GigabitEthernet1/0/2] quit

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

Verify the configuration:

# Display the DLDP configuration globally and on all the DLDP-enabled ports of Device A.
[DeviceA] display dldp
DLDP global status: Enabled
DLDP advertisement interval: 5s
DLDP authentication-mode: None
DLDP unidirectional-shutdown mode: Auto
DLDP delaydown-timer value: 1s
Number of enabled ports: 2

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

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

The output shows that both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are bidirectional.
# Enable the monitoring of logs on the current terminal on Device A. Set the lowest level of the logs that can be output to the current terminal to 6.

[DeviceA] quit
<DeviceA> terminal monitor
<DeviceA> terminal logging level 6

The following log information is displayed on Device A:

<DeviceA>% Jul 11 17:40:31:089 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is DOWN.
% Jul 11 17:40:31:091 2016 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface GigabitEthernet1/0/1 is DOWN.
% Jul 11 17:40:31:677 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is DOWN.
% Jul 11 17:40:31:678 2016 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface GigabitEthernet1/0/2 is DOWN.
% Jul 11 17:40:38:544 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is UP.
% Jul 11 17:40:38:836 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is UP.

The output shows the following:

- The port status of both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 is down and then up.
- The link status of both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 is always down.

# Display the DLDP configuration globally and of all the DLDP-enabled ports.

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

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

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

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

The unidirectional links are caused by cross-connected fibers. Correct the fiber connections. As a result, the ports shut down by DLDP automatically recover, and Device A displays the following log information:

<DeviceA>% Jul 11 17:42:57:709 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is DOWN.
% Jul 11 17:42:58:603 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is DOWN.
% Jul 11 17:43:02:342 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is UP.
Configuring the manual port shutdown mode

Network requirements

As shown in **Figure 11**, Device A and Device B are connected through two fiber pairs. Configure DLDP to detect unidirectional links. When a unidirectional link is detected, the administrator must manually shut down the port.

Figure 11 Network diagram

![Network Diagram](image)

Configuration procedure

1. Configure Device A:
   
   # Enable DLDP globally.
   
   ```
   <DeviceA> system-view
   [DeviceA] dldp enable
   ```
   
   # Configure GigabitEthernet 1/0/1 to operate in full duplex mode and at 1000 Mbps, and enable DLDP on the port.
   
   ```
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] duplex full
   [DeviceA-GigabitEthernet1/0/1] speed 1000
   [DeviceA-GigabitEthernet1/0/1] dldp enable
   ```

   # Configure GigabitEthernet 1/0/2 to operate in full duplex mode and at 1000 Mbps, and enable DLDP on the port.

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

Set the port shutdown mode to manual.

Configure Device B:

# Enable DLDP globally.

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

# Configure GigabitEthernet 1/0/2 to operate in full duplex mode and at 1000 Mbps, and enable DLDP on it.

# Set the port shutdown mode to manual.

Verify the configuration:

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

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

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

The output shows that both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are in Bidirectional state, which means both links are bidirectional.

# Enable the monitoring of logs on the current terminal on Device A. Set the lowest level of the logs that can be output to the current terminal to 6.
[DeviceA] quit
<DeviceA> terminal monitor
<DeviceA> terminal logging level 6

The following log information is displayed on Device A:

<DeviceA>%Jul 12 08:29:17:786 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is DOWN.
%Jul 12 08:29:17:787 2016 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface GigabitEthernet1/0/1 is DOWN.
%Jul 12 08:29:17:800 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is DOWN.
%Jul 12 08:29:17:800 2016 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface GigabitEthernet1/0/2 is DOWN.
%Jul 12 08:29:25:004 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is UP.
%Jul 12 08:29:25:005 2016 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface GigabitEthernet1/0/1 is UP.
%Jul 12 08:29:25:893 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is UP.

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

# Display the DLDP configuration globally and of all the DLDP-enabled ports.
<DeviceA> display dldp
DLDP global status: Enabled
DLDP advertisement interval: 5s
DLDP authentication-mode: None
DLDP unidirectional-shutdown mode: Manual
DLDP delaydown-timer value: 1s
Number of enabled ports: 2

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

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

The output shows that the DLDP port status of both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 is unidirectional. DLDP detects unidirectional links on the two ports but does not shut them down.
The unidirectional links are caused by cross-connected fibers. Manually shut down the two ports:

# Shut down GigabitEthernet 1/0/1.

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

The following log information is displayed on Device A:

[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:34:23:717 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is DOWN.
[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:34:23:718 2016 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface GigabitEthernet1/0/1 is DOWN.
[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:34:23:778 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is DOWN.

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

# Shut down GigabitEthernet 1/0/2.

[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] shutdown

Correct the fiber connections and bring up the two ports:

# Bring up GigabitEthernet 1/0/2.

[DeviceA-GigabitEthernet1/0/2] undo shutdown

The following log information is displayed on Device A:

[DeviceA-GigabitEthernet1/0/2]%Jul 12 08:46:17:677 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is UP.
[DeviceA-GigabitEthernet1/0/2]%Jul 12 08:46:17:959 2016 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed on interface GigabitEthernet1/0/2. The neighbor's system MAC is 0023-8956-3600, and the port index is 2.

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

# Bring up GigabitEthernet 1/0/1.

[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA-GigabitEthernet1/0/2] undo shutdown

The following log information is displayed on Device A:

[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:48:25:952 2016 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is UP.
[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:48:25:952 2016 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed on interface GigabitEthernet1/0/1. The neighbor's system MAC is 0023-8956-3600, and the port index is 1.
The output shows that the port status and link status of GigabitEthernet 1/0/1 are now up and its DLDP neighbors are determined.

Configuring the hybrid port shutdown mode

Network requirements

As shown in Figure 12, Device A and Device B are connected through two fiber pairs.

Configure DLDP to detect unidirectional links. When a unidirectional link is detected, DLDP automatically shuts down the unidirectional port. The administrator needs to bring up the port after clearing the fault.

Figure 12 Network diagram

Configuration procedure

1. Configure Device A:

   # Enable DLDP globally.
   <DeviceA> system-view
   [DeviceA] dldp enable

   # Configure GigabitEthernet 1/0/1 to operate in full duplex mode and at 1000 Mbps, and enable DLDP on the port.
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] duplex full
   [DeviceA-GigabitEthernet1/0/1] speed 1000
   [DeviceA-GigabitEthernet1/0/1] dldp enable
   [DeviceA-GigabitEthernet1/0/1] quit

   # Configure GigabitEthernet 1/0/2 to operate in full duplex mode and at 1000 Mbps, and enable DLDP on the port.
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] duplex full
   [DeviceA-GigabitEthernet1/0/2] speed 1000
   [DeviceA-GigabitEthernet1/0/2] dldp enable
   [DeviceA-GigabitEthernet1/0/2] quit

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

2. Configure Device B:

   # Enable DLDP globally.
   <DeviceB> system-view
   [DeviceB] dldp global enable

   # Configure GigabitEthernet 1/0/1 to operate in full duplex mode and at 1000 Mbps, and enable DLDP on it.
   [DeviceB] interface gigabitethernet 1/0/1
# Configure GigabitEthernet 1/0/2 to operate in full duplex mode and at 1000 Mbps, and enable DLDP on it.
[DeviceB-GigabitEthernet1/0/2] duplex full
[DeviceB-GigabitEthernet1/0/2] speed 1000
[DeviceB-GigabitEthernet1/0/2] dldp enable
[DeviceB-GigabitEthernet1/0/2] quit

# Set the port shutdown mode to hybrid.
[DeviceB] dldp unidirectional-shutdown hybrid

Verifying the configuration

# Display the DLDP configuration globally and on all the DLDP-enabled ports of Device A.
[DeviceA] display dldp
DLDP global status: Enabled
DLDP advertisement interval: 5s
DLDP authentication-mode: None
DLDP unidirectional-shutdown mode: Manual
DLDP delaydown-timer value: 1s
Number of enabled ports: 2

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

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

The output shows that both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are in Bidirectional state, which means both links are bidirectional.

# Enable the monitoring of logs on the current terminal on Device A. Set the lowest level of the logs that can be output to the current terminal to 6.
[DeviceA] quit
<DeviceA> terminal monitor
<DeviceA> terminal logging level 6

The following log information is displayed on Device A:
<DeviceA>%Jan  4 07:16:06:556 2011 DeviceA DLDP/5/DLDP_NEIGHBOR_AGED: A neighbor on interface
GigabitEthernet1/0/1 was deleted because the neighbor was aged. The neighbor's system MAC is 0023-8956-3600, and the port index is 162.

%Jan 4 07:16:06:560 2011 DeviceA DLDP/5/DLDP_NEIGHBOR_AGED: A neighbor on interface GigabitEthernet1/0/2 was deleted because the neighbor was aged. The neighbor's system MAC is 0023-8956-3600, and the port index is 165.


%Jan 4 07:16:07:152 2011 DeviceA DLDP/3/DLDP_LINK_UNIDIRECTIONAL: DLDP detected a unidirectional link on interface GigabitEthernet1/0/1. DLDP automatically shut down the interface. Please manually bring up the interface.
%Jan 4 07:16:07:156 2011 DeviceA DLDP/3/DLDP_LINK_UNIDIRECTIONAL: DLDP detected a unidirectional link on interface GigabitEthernet1/0/2. DLDP automatically shut down the interface. Please manually bring up the interface.

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

# Display the DLDP configuration globally and of all the DLDP-enabled ports.
<DeviceA> display dldp
DLDP global status: Enabled
DLDP advertisement interval: 5s
DLDP authentication-mode: None
DLDP unidirectional-shutdown mode: Hybrid
DLDP delaydown-timer value: 1s
Number of enabled ports: 2

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

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

The output shows that DLDP detects a unidirectional link and shuts down GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

The unidirectional links are caused by cross-connected fibers. Bring up the two ports after correct the fiber connection:

# Bring up GigabitEthernet 1/0/1.
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo shutdown

The following log information is displayed on Device A:
%Jan 4 07:33:57:562 2011 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed on interface GigabitEthernet1/0/1. The neighbor's system MAC is 0023-8956-3600, and the port index is 162.
%Jan 4 07:33:57:609 2011 DeviceA STP/6/STP_DETECTED_TC: Instance 0's port GigabitEthernet1/0/1 detected a topology change.

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

# Bring up GigabitEthernet 1/0/2.

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

The following log information is displayed on Device A:

%Jan 4 07:35:57:562 2011 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed on interface GigabitEthernet1/0/2. The neighbor's system MAC is 0023-8956-3600, and the port index is 162.
%Jan 4 07:35:57:609 2011 DeviceA STP/6/STP_DETECTED_TC: Instance 0's port GigabitEthernet1/0/2 detected a topology change.

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

Overview

Metropolitan area networks (MANs) and enterprise networks typically use the ring topology to improve reliability. However, services will be interrupted if any node in the ring network fails. A ring network typically uses RPR or Ethernet rings. RPR is high in cost because it needs dedicated hardware. In contrast, the Ethernet ring technology is more mature and economical, so it is more and more popular in MANs and enterprise networks.

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. RRPP can also rapidly restore the communication paths between the nodes when a link is disconnected on the ring. The convergence time of RRPP is independent of the number of nodes in the Ethernet ring. RRPP is applicable to large-diameter networks.

Basic RRPP concepts

Figure 13 shows a typical RRPP network with two Ethernet rings and multiple nodes. RRPP detects ring status and sends topology change information by exchanging Rapid Ring Protection Protocol Data Units (RRPPDUs) among the nodes.

Figure 13 RRPP networking diagram

RRPP domain

An RRPP domain is uniquely identified by a domain ID. The interconnected devices with the same domain ID and control VLANs constitute an RRPP domain. An RRPP domain contains the following elements:

- Primary ring and subring.
- Control VLAN.
- Master node, transit node, edge node, and assistant edge node.
- Primary port, secondary port, common port, and edge port.

As shown in Figure 13, Domain 1 is an RRPP domain, containing two RRPP rings: Ring 1 and Ring 2. All the nodes on the two RRPP rings belong to the RRPP domain.
A ring-shaped Ethernet topology is called an RRPP ring. RRPP rings include primary rings and subrings. 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 physical links on the Ethernet ring are connected.
- **Disconnect state**—Some physical links on the Ethernet ring are not connected.

As shown in Figure 13, Domain 1 contains two RRPP rings: Ring 1 and Ring 2. The level is set to 0 for Ring 1 and 1 for Ring 2. Ring 1 is configured as the primary ring, and Ring 2 is configured as a subring.

**Control VLAN and protected VLAN**

1. **Control VLAN**

   In an RRPP domain, a control VLAN is dedicated to transferring RRPPDUs. On a device, the ports accessing an RRPP ring belong to the control VLANs of the ring, and only these ports can join the control VLANs.

   An RRPP domain is configured with the following control VLANs:
   - One primary control VLAN, which is the control VLAN for the primary ring.
   - One secondary control VLAN, which is the control VLAN for subrings.

   After you specify a VLAN as the primary control VLAN, the system automatically configures the secondary control VLAN. The VLAN ID is the primary control VLAN ID plus one. All subrings in the same RRPP domain share the same secondary control VLAN. IP address configuration is prohibited on the control VLAN interfaces.

2. **Protected VLAN**

   A protected VLAN is dedicated to transferring data packets. Both RRPP ports and non-RRPP ports can be assigned to a protected 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 only one master node. The master node initiates the polling mechanism and determines the operations to be performed after a topology change.

- **Transit node**—On the primary ring, transit nodes refer to all nodes except the master node. On the subring, transit nodes refer to all nodes except the master node and the nodes where the primary ring intersects with the subring. 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 determines 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 acts as a master node or transit node on the primary ring and as 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 acts as a master node or transit node on the primary ring and as 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 13, Ring 1 is the primary ring and Ring 2 is a subring. Device A is the master node of Ring 1. 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.

**Port**

1. **Primary port and secondary port**
Each master node or transit node has two ports connected to an RRPP ring, a primary port and a secondary port. You can determine the role of a port.

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 Hello packets, respectively.
- When an RRPP ring is in Health state, the secondary port logically denies protected VLANs and permits only the packets from the control VLANs.
- When an RRPP ring is in Disconnect state, the secondary port forwards packets from protected VLANs.

In terms of functionality, the primary port and the secondary port of a transit node are the same. Both are designed for transferring protocol packets and data packets over an RRPP ring.

As shown in Figure 13, 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.

2. 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. You can determine the role of a port.

As shown in Figure 13, Device B and Device C reside 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. 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). 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. An RRPP ring group configured on an assistant edge node is an assistant edge node RRPP ring group. Only one subring in an edge node RRPP ring group is allowed to send Edge-Hello packets.

RRPPDUs

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.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>The master node sends Hello packets (also known as Health packets) to detect the integrity of a ring in a network.</td>
</tr>
<tr>
<td>Link-Down</td>
<td>When a port on the transit node, edge node, or assistant edge node fails, the node initiates Link-Down packets to notify the master node of the disconnection of the ring.</td>
</tr>
<tr>
<td>Common-Flush-FDB</td>
<td>When an RRPP ring transits to Disconnect state, the master node initiates Common-Flush-FDB (FDB stands for Forwarding Database) packets. It uses the packets to instruct the transit nodes, edge nodes, and assistant edge nodes to update their own MAC address entries and ARP/ND entries.</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Complete-Flush-FDB</td>
<td>When an RRPP ring transits to Health state, the master node sends Complete-Flush-FDB packets for the following purposes:</td>
</tr>
<tr>
<td></td>
<td>• Instruct the transit nodes, edge nodes, and assistant edge nodes to update their MAC address entries and ARP/ND entries.</td>
</tr>
<tr>
<td></td>
<td>• Instruct the transit nodes to unblock temporarily blocked ports.</td>
</tr>
<tr>
<td>Edge-Hello</td>
<td>The edge node sends Edge-Hello packets to examine the SRPTs between the edge node and the assistant edge node.</td>
</tr>
<tr>
<td>Major-Fault</td>
<td>The assistant edge node sends Major-Fault packets to notify the edge node of SRPT failure when an SRPT between assistant edge node and edge node is disconnected.</td>
</tr>
</tbody>
</table>

**RRPP timers**

When RRPP determines the link state of an Ethernet ring, it uses the following timers:

- **Hello timer**—Specifies the interval at which the master node sends Hello packets out of the primary port.
- **Fail timer**—Specifies the maximum delay of Hello packets sent from the primary port to the secondary port of the master node. If the secondary port receives the Hello packets sent by the local master node before the Fail timer expires, the ring is in Health state. Otherwise, the ring transits to Disconnect state.

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

**How RRPP works**

**Polling mechanism**

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

The master node sends Hello packets out of its primary port at the Hello interval. 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 receives Hello packets before the Fail timer expires. The master node keeps the secondary port blocked.
- If the ring is disconnected, the secondary port of the master node fails to receive Hello packets before the Fail timer expires. The master node releases the secondary port from blocking protected VLANs. It sends Common-Flush-FDB packets to instruct all transit nodes to update their own MAC address entries and ARP/ND entries.

**Load balancing**

In a ring network, traffic from multiple VLANs might be transmitted at the same time. RRPP can implement load balancing by transmitting traffic from different VLANs along different paths.

You can configure multiple RRPP domains for a ring network. Each RRPP domain transmits the traffic from the specified VLANs (protected VLANs). Traffic from different VLANs can be transmitted according to different topologies in the ring network for load balancing.

As shown in **Figure 18**, 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. Device B is the master node of Ring 1 in Domain 2. With such configurations, traffic from different VLANs can be transmitted on different links for load balancing in the single-ring network.
Link down alarm mechanism

In an RRPP domain, when the transit node, edge node, or assistant edge node finds that any of its ports is down, it immediately sends Link-Down packets to the master node. When the master node receives a Link-Down packet, it takes the following actions:

- Releases the secondary port from blocking protected VLANs.
- Sends Common-Flush-FDB packets to instruct all the transit nodes, edge nodes, and assistant edge nodes to update their MAC address entries and ARP/ND entries.

After each node updates its own entries, traffic is switched to the normal link.

Ring recovery

When the ports in an RRPP domain on the transit nodes, edge nodes, or assistant edge nodes come up again, the ring is recovered. However, the master node might detect the ring recovery after a period of time. A temporary loop might arise in the protected VLAN during this period. As a result, a broadcast storm occurs.

To prevent such cases, non-master nodes block the ports immediately when they find the ports accessing the ring are brought up again. The nodes block only the packets from the protected VLAN, and they permit only the packets from the control VLAN to pass through. The blocked ports are activated only when the nodes determine that no loop will be generated by these ports.

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

As shown in Figure 17, 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 secondary ports. A loop is generated among Device B, Device C, Device E, and Device F, causing a broadcast storm.

To avoid generating a loop, the edge node will temporarily block the edge port. The blocked edge port is activated only when the edge node determines that no loop will be generated when the edge port is activated.

RRPP ring group

In an edge node RRPP ring group, only the activated subring with the smallest 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.

When an edge node RRPP ring group and an assistant edge node RRPP ring group are configured, the CPU workload is reduced because of the following reasons:

- Only one subring sends Edge-Hello packets on the edge node.
- Only one subring receives Edge-Hello packets on the assistant edge node.

As shown in Figure 17, Device B is the edge node of Ring 2 and Ring 3. Device C is the assistant edge node of Ring 2 and Ring 3. Device B and Device C need to send or receive Edge-Hello packets frequently. If more subrings are configured or more domains are configured for load balancing, Device B and Device C will send or receive a large number of Edge-Hello packets.

To reduce Edge-Hello traffic, perform the following tasks:

- Assign Ring 2 and Ring 3 to an RRPP ring group configured on the edge node Device B.
- Assign Ring 2 and Ring 3 to an RRPP ring group configured on the assistant edge node Device C.

If all rings are activated, only Ring 2 on Device B sends Edge-Hello packets.

Typical RRPP networking

Single ring

As shown in Figure 14, only a single ring exists in the network topology. You need only define an RRPP domain.
**Figure 14** Schematic diagram for a single-ring network

![Single-ring network diagram](image)

Tangent rings

As shown in **Figure 15**, two or more rings exist in the network topology and only one common node exists between rings. You must define an RRPP domain for each ring.

**Figure 15** Schematic diagram for a tangent-ring network

![Tangent-ring network diagram](image)

Intersecting rings

As shown in **Figure 16**, two or more rings exist in the network topology and two common nodes exist between rings. You need only define an RRPP domain and configure one ring as the primary ring and the other rings as subrings.
**Figure 16** Schematic diagram for an intersecting-ring network

As shown in Figure 17, two or more rings exist in the network topology and two similar common nodes exist between rings. You need only define an RRPP domain and configure one ring as the primary ring and the other rings as subrings.

**Figure 17** Schematic diagram for a dual-homed-ring network

**Dual-homed rings**

As shown in Figure 17, two or more rings exist in the network topology and two similar common nodes exist between rings. You need only define an RRPP domain and configure one ring as the primary ring and the other rings as subrings.

**Figure 17** 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 18:

- 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 achieve single-ring load balancing.
Intersecting-ring load balancing

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

As shown in Figure 19:

- 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.

Traffic from different VLANs can travel over different paths in the subring and primary ring.

Protocols and standards

RFC 3619, Extreme Networks’ Ethernet Automatic Protection Switching (EAPS) Version 1
RRPP configuration task list

You can configure RRPP in the following order:

- Create RRPP domains based on service planning.
- Specify control VLANs and protected VLANs for each RRPP domain.
- Determine the ring roles and node roles based on the traffic paths in each RRPP domain.

RRPP does not have an auto election mechanism. You must configure each node in the ring network correctly for RRPP to monitor and protect the ring network.

Before you configure RRPP, you must physically construct a ring-shaped Ethernet topology.

To configure RRPP, perform the following tasks:

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Creating an RRPP domain</td>
<td>Perform this task on all nodes in the RRPP domain.</td>
</tr>
<tr>
<td>(Required.) Configuring control VLANs</td>
<td>Perform this task on all nodes in the RRPP domain.</td>
</tr>
<tr>
<td>(Required.) Configuring protected VLANs</td>
<td>Perform this task on all nodes in the RRPP domain.</td>
</tr>
<tr>
<td>(Required.) Configuring RRPP rings:</td>
<td>Perform this task on all nodes in the RRPP domain.</td>
</tr>
<tr>
<td>- Configuring RRPP ports</td>
<td></td>
</tr>
<tr>
<td>- Configuring RRPP nodes</td>
<td></td>
</tr>
<tr>
<td>(Required.) Activating an RRPP domain</td>
<td>Perform this task on all nodes in the RRPP domain.</td>
</tr>
<tr>
<td>(Optional.) Configuring RRPP timers</td>
<td>Perform this task on the master node in the RRPP domain.</td>
</tr>
<tr>
<td>(Optional.) Configuring an RRPP ring group</td>
<td>Perform this task on the edge node and assistant edge node in the RRPP domain.</td>
</tr>
<tr>
<td>(Optional.) Enabling SNMP notifications for RRPP</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Creating an RRPP domain

When you create an RRPP domain, specify a domain ID to uniquely identify the RRPP domain. All devices in the same RRPP domain must be configured with the same domain ID.

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

To create an RRPP domain:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>rrpp domain domain-id</td>
<td>By default, no RRPP domains exist.</td>
</tr>
</tbody>
</table>

Configuring control VLANs

Before you configure RRPP rings in an RRPP domain, configure the same control VLANs for all nodes in the RRPP domain first. You need only configure the primary control VLAN for an RRPP domain. The system automatically configures the secondary control VLAN. 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 previously assigned.

Follow these guidelines when you configure control VLANs:

- Do not configure the default VLAN of a port accessing an RRPP ring as the control VLAN, and do not enable QinQ or VLAN mapping on control VLANs. If you do, RRPPDUs cannot be correctly forwarded.
- After you configure RRPP rings for an RRPP domain, you cannot delete or modify the primary control VLAN of the domain. You can only use the `undo control-vlan` command to delete a primary control VLAN.
- To transparently transmit RRPPDUs on a device not configured with RRPP, make sure only the two ports accessing the RRPP ring permit packets from the control VLANs. Otherwise, the packets from other VLANs might enter the control VLANs in transparent transmission mode and strike the RRPP ring.

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

To configure control VLANs:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter RRPP domain view</td>
<td><code>rrpp domain domain-id</code></td>
</tr>
<tr>
<td>3.</td>
<td>Configure the primary control VLAN for the RRPP domain.</td>
<td><code>control-vlan vlan-id</code>&lt;br&gt;By default, no control VLAN exists in an RRPP domain.</td>
</tr>
</tbody>
</table>

### Configuring protected VLANs

Before you configure RRPP rings in an RRPP domain, configure the same protected VLANs for all nodes in the RRPP domain. All VLANs to which the RRPP ports are assigned must be protected by the RRPP domains.

Protected VLANs are configured by referencing Multiple Spanning Tree Instances (MSTIs). The protected VLAN configuration method varies by the spanning tree mode:

- In STP, RSTP, or MSTP mode, you must manually configure the mappings between VLANs and MSTIs.
- In PVST mode, the device automatically maps each VLAN to an MSTI. When the spanning tree protocol is disabled globally, all VLANs are automatically mapped to MSTI 0.

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

**IMPORTANT:**

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

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

To configure protected VLANs:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>2.</td>
<td>stp region-configuration</td>
<td>Not required if the device is operating in PVST mode. For more information about the command, see Layer 2—LAN Switching Command Reference.</td>
</tr>
</tbody>
</table>
| 3.   | • Method 1: instance instance-id vlan vlan-id-list  
• Method 2: vlan-mapping modulo modulo | By default, all VLANs in an MST region are mapped to MSTI 0 (the CIST). Not required if the device is operating in PVST mode. For more information about the commands, see Layer 2—LAN Switching Command Reference. |
| 4.   | 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. |
| 5.   | display stp region-configuration | Available in any view. The output of the command includes VLAN-to-instance mappings. For more information about the command, see Layer 2—LAN Switching Command Reference. |
| 6.   | quit | Not required if the device is operating in PVST mode. |
| 7.   | rrpp domain domain-id | N/A |
| 8.   | protected-vlan reference-instance instance-id-list | By default, no protected VLANs exist in an RRPP domain. |

### Configuring RRPP rings

When you configure an RRPP ring, you must configure the ports connecting each node to the RRPP ring before configuring the nodes.

### Configuring RRPP ports

Follow these guidelines when you configure RRPP ports:

- Do not enable the OAM remote loopback function on an RRPP port. Otherwise, temporary broadcast storms might occur.
- To accelerate topology convergence, use the `link-delay` command to set the physical state change suppression interval to 0 seconds. For more information about the `link-delay` command, see Interface Command Reference.

Perform this task on each node’s ports intended for accessing RRPP rings.

To configure RRPP ports:
### Configuring RRPP nodes

The maximum number of rings that can be configured on a device in all RRPP domains is 64.

If a device carries multiple RRPP rings in an RRPP domain, it can only be an edge node or an assistant edge node on a subring.

#### Specifying a master node

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RRPP domain view.</td>
<td>rrpp domain domain-id</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the current device as the master node of the ring, and specify the primary port and the secondary port.</td>
<td>ring ring-id node-mode master [ primary-port interface-type interface-number ] [ secondary-port interface-type interface-number ] level level-value</td>
</tr>
</tbody>
</table>

#### Specifying a transit node

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RRPP domain view.</td>
<td>rrpp domain domain-id</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the current device as a transit node of the ring, and specify the primary port and the secondary port.</td>
<td>ring ring-id node-mode transit [ primary-port interface-type interface-number ] [ secondary-port interface-type interface-number ] level level-value</td>
</tr>
</tbody>
</table>
Specifying an edge node

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

To specify an edge node:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RRPP domain view.</td>
<td>rrp domain domain-id</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the current device as a master node or transit node of the primary ring, and specify the primary port and the secondary port.</td>
<td>ring ring-id node-mode { master</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the current device as the edge node of a subring, and specify the edge port.</td>
<td>ring ring-id node-mode edge [ edge-port interface-type interface-number ]</td>
</tr>
</tbody>
</table>

Specifying an assistant edge node

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

To specify an assistant edge node:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RRPP domain view.</td>
<td>rrp domain domain-id</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the current device as a master node or transit node of the primary ring, and specify the primary port and the secondary port.</td>
<td>ring ring-id node-mode { master</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the current device as the assistant edge node of the subring, and specify an edge port.</td>
<td>ring ring-id node-mode assistant-edge [ edge-port interface-type interface-number ]</td>
</tr>
</tbody>
</table>

Activating an RRPP domain

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

Follow these guidelines when you activate an RRPP domain:

- Before you enable subrings on a device, you must enable the primary ring. Before you disable the primary ring on the device, you must disable all subrings. Otherwise, the system displays error prompts.
- To prevent Hello packets of subrings from being looped on the primary ring, enable the primary ring on its master node first. Then enable the subrings on their respective master nodes.
Perform this task on all nodes in the RRPP domain.

To activate an RRPP domain:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>rrpp enable</td>
<td>By default, RRPP is disabled.</td>
</tr>
<tr>
<td>3.</td>
<td>rrpp domain domain-id</td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>ring ring-id enable</td>
<td>By default, an RRPP ring is disabled.</td>
</tr>
</tbody>
</table>

## Configuring RRPP timers

The Fail timer must be greater than or equal to three times the Hello timer.

In a dual-homed-ring network, make sure the difference between the Fail timer values on the master node of the subring and the master node of the primary ring is greater than twice the Hello timer value on the master node of the subring. Otherwise, temporary loops might occur when the primary ring fails.

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

To configure RRPP timers:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>rrpp domain domain-id</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>timer hello-timer hello-value fail-timer fail-value</td>
<td>By default, the Hello timer value is 1 second and the Fail timer value is 3 seconds.</td>
</tr>
</tbody>
</table>

## Configuring an RRPP ring group

To reduce Edge-Hello traffic, assign subrings with the same edge node and 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. It can only be configured on these two types of nodes.

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

Follow these guidelines when you configure an RRPP ring group:

- You can assign a subring to only one RRPP ring group. The RRPP ring groups configured on the edge node and the assistant edge node must contain the same subrings. Otherwise, the RRPP ring group cannot operate correctly.
- The subrings in an RRPP ring group must share the same edge node and assistant edge node. The edge node and the assistant edge node must have the same SRPTs.
- Make sure a device is either the edge node or the assistant edge node on the subrings in an RRPP ring group.
- Make sure the RRPP ring groups on the edge node and the assistant edge node have the same configurations and activation status.
- Make sure all subrings in an RRPP ring group have the same SRPTs. If the SRPTs of these subrings are different, the RRPP ring group cannot operate correctly.
To configure an RRPP ring group:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>rrpp ring-group ring-group-id</td>
<td>By default, no RRPP ring groups exist.</td>
</tr>
<tr>
<td>3.</td>
<td>domain domain-id ring ring-id-list</td>
<td>By default, no subrings are assigned to an RRPP ring group.</td>
</tr>
</tbody>
</table>

Enabling SNMP notifications for RRPP

To report critical RRPP events to an NMS, enable SNMP notifications for RRPP. For RRPP event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

To enable SNMP notifications for RRPP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>snmp-agent trap enable rrpp [ major-fault</td>
<td>multi-master</td>
</tr>
</tbody>
</table>

Displaying and maintaining RRPP

Execute `display` commands in any view and `reset` commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display brief RRPP information.</td>
<td>display rrpp brief</td>
</tr>
<tr>
<td>Display RRPP group configuration information.</td>
<td>display rrpp ring-group [ ring-group-id ]</td>
</tr>
<tr>
<td>Display RRPPDU statistics.</td>
<td>display rrpp statistics domain domain-id [ ring ring-id ]</td>
</tr>
<tr>
<td>Display detailed RRPP information.</td>
<td>display rrpp verbose domain domain-id [ ring ring-id ]</td>
</tr>
<tr>
<td>Clear RRPPDU statistics.</td>
<td>reset rrpp statistics domain domain-id [ ring ring-id ]</td>
</tr>
</tbody>
</table>

RRPP configuration examples

Single ring configuration example

Network requirements

As shown in Figure 20:
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. Specify the protected VLANs of RRPP domain 1 as 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 GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port on Device B, Device C, and Device D.

**Figure 20 Network diagram**

---

**Configuration procedure**

1. Configure Device A:

   - # Create VLANs 1 through 30.
   
   ```
   <DeviceA> system-view
   [DeviceA] vlan 1 to 30
   ```

   - # Map these VLANs to MSTI 1.
   
   ```
   [DeviceA] stp region-configuration
   [DeviceA-mst-region] instance 1 vlan 1 to 30
   ```

   - # Activate the MST region configuration.
   
   ```
   [DeviceA-mst-region] active region-configuration
   [DeviceA-mst-region] quit
   ```

   - # Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
   
   ```
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] link-delay 0
   ```

   - # Disable the spanning tree feature on the port.
   
   ```
   [DeviceA-GigabitEthernet1/0/1] undo stp enable
   ```

   - # Configure the port as a trunk port.
   
   ```
   [DeviceA-GigabitEthernet1/0/1] port link-type trunk
   ```

   - # Assign the port to VLANs 1 through 30.
   
   ```
   [DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
   [DeviceA-GigabitEthernet1/0/1] quit
   ```

   - # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
   
   ```
   [DeviceA] interface gigabitethernet 1/0/2
   ```
DeviceA-GigabitEthernet1/0/2] link-delay 0
DeviceA-GigabitEthernet1/0/2] undo stp enable
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.
DeviceA] rrpp domain 1

# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
DeviceA-rrpp-domain1] control-vlan 4092

# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
DeviceA-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
DeviceA-rrpp-domain1] ring 1 enable
DeviceA-rrpp-domain1] quit

# Enable RRPP.
DeviceA] rrpp enable

2. Configure Device B:

# Create VLANs 1 through 30.
<DeviceB> system-view
[DeviceB] vlan 1 to 30

# Map these VLANs to MSTI 1.
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30

# Activate the MST region configuration.
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceB-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceB-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 1 through 30.
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[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.
[DeviceB] rrpp domain 1
# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceB-rrpp-domain1] control-vlan 4092
# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
# Configure Device B as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
[DeviceB-rrpp-domain1] quit
# Enable RRPP.
[DeviceB] rrpp enable
3. Configure Device C:
   Configure Device C in the same way Device B is configured.
4. Configure Device D:
   Configure Device D in the same way Device B is configured.

Verifying the configuration

# Use the display commands to view RRPP configuration and operational information on each device.

Intersecting ring configuration example

Network requirements

As shown in Figure 21:

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

1. Configure Device A:
   # Create VLANs 1 through 30.
   [DeviceA] system-view
   [DeviceA] vlan 1 to 30
   # Map these VLANs to MSTI 1.
   [DeviceA-mst-region] instance 1 vlan 1 to 30
   # Activate the MST region configuration.
   [DeviceA-mst-region] active region-configuration
   [DeviceA-mst-region] quit
   # Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
   [DeviceA-GigabitEthernet1/0/1] link-delay 0
   # Disable the spanning tree feature on the port.
   [DeviceA-GigabitEthernet1/0/1] undo stp enable
   # Configure the port as a trunk port.
   [DeviceA-GigabitEthernet1/0/1] port link-type trunk
   # Assign the port to VLANs 1 through 30.
   [DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
   [DeviceA-GigabitEthernet1/0/1] quit
   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
   [DeviceA-GigabitEthernet1/0/2] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] link-delay 0
   [DeviceA-GigabitEthernet1/0/2] undo stp enable
   [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.
   [DeviceA-GigabitEthernet1/0/1] rrpp domain 1
   # Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
   [DeviceA-rrpp-domain1] control-vlan 4092
# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit

# Enable RRPP.
[DeviceA] rrpp enable

2. Configure Device B:

# Create VLANs 1 through 30.
<DeviceB> system-view
[DeviceB] vlan 1 to 30

# Map these VLANs to MSTI 1.
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30

# Activate the MST region configuration.
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceB-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceB-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 1 through 30.
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] quit

# Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] link-delay 0
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[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.
[DeviceB] rrpp domain 1

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

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

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

# Enable RRPP.

3. Configure Device C:

# Create VLANs 1 through 30.

# Map these VLANs to MSTI 1.

# Activate the MST region configuration.

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

# Disable the spanning tree feature on the port.

# Configure the port as a trunk port.

# Assign the port to VLANs 1 through 30.

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

# Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.
# Create RRPP domain 1.
[DeviceC] rrrp domain 1

# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceC-rrrp-domain1] control-vlan 4092

# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceC-rrrp-domain1] protected-vlan reference-instance 1

# Configure Device C as a transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceC-rrrp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrrp-domain1] ring 1 enable

# Configure Device C as the assistant edge node of subring 2, with GigabitEthernet 1/0/3 as the edge port. Enable ring 2.
[DeviceC-rrrp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceC-rrrp-domain1] ring 2 enable

# Enable RRPP.
[DeviceC] rrrp enable

4. Configure Device D:

# Create VLANs 1 through 30.
<DeviceD> system-view
[DeviceD] vlan 1 to 30

# Map these VLANs to MSTI 1.
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30

# Activate the MST region configuration.
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceD-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceD-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 1 through 30.
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] link-delay 0
[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 RRPP domain 1.
[DeviceD] rrpp domain 1
# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceD-rrpp-domain1] control-vlan 4092
# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
# Configure Device D as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
[DeviceD-rrpp-domain1] quit
# Enable RRPP.
[DeviceD] rrpp enable
5. Configure Device E:
# Create VLANs 1 through 30.
<DeviceE> system-view
[DeviceE] vlan 1 to 30
# Map these VLANs to MSTI 1.
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 1 vlan 1 to 30
# Activate the MST region configuration.
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] link-delay 0
# Disable the spanning tree feature on the port.
[DeviceE-GigabitEthernet1/0/1] undo stp enable
# Configure the port as a trunk port.
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
# Assign the port to VLANs 1 through 30.
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/1] quit
# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] link-delay 0
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[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.
[DeviceE] rrpp domain 1
# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceE-rrpp-domain1] control-vlan 4092
# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceE-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device E as the master node of subring 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 2.
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1
[DeviceE-rrpp-domain1] ring 2 enable
[DeviceE-rrpp-domain1] quit

# Enable RRPP.
[DeviceE] rrpp enable

Verifying the configuration
# Use the display commands to view RRPP configuration and operational information on each device.

Dual-homed rings configuration example

Network requirements

As shown in Figure 22:

• Device A through Device H form RRPP domain 1. Specify the primary control VLAN of RRPP domain 1 as VLAN 4092. Specify the protected VLANs of RRPP domain 1 as VLANs 1 through 30.


• Specify Device A, Device E, Device F, Device G, and Device H as the master nodes of Ring 1, Ring 2, Ring 3, Ring 4, and Ring 5, respectively. Specify GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port on the rings.

• 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.

IMPORTANT:
Configure the primary and secondary ports on the master nodes correctly to make sure other protocols still operate correctly when protected VLANs are denied by the secondary ports.
Configuration procedure

1. Configure Device A:
   # Create VLANs 1 through 30.
   <DeviceA> system-view
   [DeviceA] vlan 1 to 30
   # Map these VLANs to MSTI 1.
   [DeviceA] stp region-configuration
   [DeviceA-mst-region] instance 1 vlan 1 to 30
   # Activate the MST region configuration.
   [DeviceA-mst-region] active region-configuration
   [DeviceA-mst-region] quit
   # Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] link-delay 0
   # Disable the spanning tree feature on the port.
   [DeviceA-GigabitEthernet1/0/1] undo stp enable
   # Configure the port as a trunk port.
   [DeviceA-GigabitEthernet1/0/1] port link-type trunk
   # Assign the port to VLANs 1 through 30.
   [DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
   [DeviceA-GigabitEthernet1/0/1] quit
   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] link-delay 0
   [DeviceA-GigabitEthernet1/0/2] undo stp enable
   [DeviceA-GigabitEthernet1/0/2] port link-type trunk
   [DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
   [DeviceA-GigabitEthernet1/0/2] quit
# Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] link-delay 0
[DeviceA-GigabitEthernet1/0/3] undo stp enable
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/3] quit

# Configure GigabitEthernet 1/0/4 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] link-delay 0
[DeviceA-GigabitEthernet1/0/4] undo stp enable
[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.
[DeviceA] rrpp domain 1

# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceA-rrpp-domain1] control-vlan 4092

# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable

# Configure Device A as the edge node of subring 2, with GigabitEthernet 1/0/4 as the edge port. Enable subring 2.
[DeviceA-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceA-rrpp-domain1] ring 2 enable

# Configure Device A as the edge node of subring 3, with GigabitEthernet 1/0/3 as the edge port. Enable subring 3.
[DeviceA-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceA-rrpp-domain1] ring 3 enable
[DeviceA-rrpp-domain1] quit

# Enable RRPP.
[DeviceA] rrpp enable

2. Configure Device B:
# Create VLANs 1 through 30.
<DeviceB> system-view
[DeviceB] vlan 1 to 30

# Map these VLANs to MSTI 1.
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30

# Activate the MST region configuration.
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceB] interface gigabitethernet 1/0/1
# Disable the spanning tree feature on the port.
[DeviceB-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceB-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 1 through 30.
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceB-GigabitEthernet1/0/2] interface gigabitethernet 1/0/2

# Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceB-GigabitEthernet1/0/3] interface gigabitethernet 1/0/3

# Configure GigabitEthernet 1/0/4 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceB-GigabitEthernet1/0/4] interface gigabitethernet 1/0/4

# Create RRPP domain 1.
[DeviceB] rrpp domain 1

# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceB-rrpp-domain1] control-vlan 4092

# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device B as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable

# Configure Device B as the assistant edge node of subring 2, with GigabitEthernet 1/0/4 as the edge port. Enable subring 2.
[DeviceB-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/4
[DeviceB-rrpp-domain1] ring 2 enable

# Configure Device B as the assistant edge node of subring 3, with GigabitEthernet 1/0/3 as the edge port. Enable subring 3.
[DeviceB-rrpp-domain1] ring 3 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceB-rrpp-domain1] ring 3 enable
[DeviceB-rrpp-domain1] quit

# Enable RRPP.
[DeviceB] rrpp enable

3. Configure Device C:
# Create VLANs 1 through 30.
<DeviceC> system-view
[DeviceC] vlan 1 to 30

# Map these VLANs to MSTI 1.
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30

# Activate the MST region configuration.
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceC-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceC-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 1 through 30.
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] link-delay 0
[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

# Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] link-delay 0
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/3] quit

# Configure GigabitEthernet 1/0/4 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] link-delay 0
[DeviceC-GigabitEthernet1/0/4] undo stp enable
[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.
[DeviceC] rrpp domain 1

# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceC-rrpp-domain1] control-vlan 4092

# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device C as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable

# Configure Device C as the assistant edge node of subring 4, with GigabitEthernet 1/0/3 as the edge port. Enable subring 4.
[DeviceC-rrpp-domain1] ring 4 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain1] ring 4 enable

# Configure Device C as the assistant edge node of subring 5, with GigabitEthernet 1/0/4 as the edge port. Enable subring 5.
[DeviceC-rrpp-domain1] ring 5 node-mode assistant-edge edge-port gigabitethernet 1/0/4
[DeviceC-rrpp-domain1] ring 5 enable

# Enable RRPP.
[DeviceC] rrpp enable

4. Configure Device D:

# Create VLANs 1 through 30.
<DeviceD> system-view
[DeviceD] vlan 1 to 30

# Map these VLANs to MSTI 1.
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30

# Activate the MST region configuration.
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceD-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceD-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 1 through 30.
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] link-delay 0
[DeviceD-GigabitEthernet1/0/2] undo stp enable
Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```plaintext
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/2] quit
```  

# Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.

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

# Configure GigabitEthernet 1/0/4 in the same way GigabitEthernet 1/0/1 is configured.

```plaintext
[DeviceD] interface gigabitethernet 1/0/4
[DeviceD-GigabitEthernet1/0/4] link-delay 0
[DeviceD-GigabitEthernet1/0/4] undo stp enable
[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.

```plaintext
[DeviceD] rrpp domain 1
```  

# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.

```plaintext
[DeviceD-rrpp-domain1] control-vlan 4092
```  

# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```plaintext
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```  

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

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

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

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

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

```plaintext
[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.

```plaintext
[DeviceD] rrpp enable
```  

5. Configure Device E:

# Create VLANs 1 through 30.

```plaintext
<DeviceE> system-view
[DeviceE] vlan 1 to 30
```  

# Map these VLANs to MSTI 1.

```plaintext
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 1 vlan 1 to 30
```  

# Activate the MST region configuration.

```plaintext
[DeviceE-mst-region] active region-configuration
```
# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceE-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceE-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 1 through 30.
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] link-delay 0
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[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.
[DeviceE] rrpp domain 1

# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceE-rrpp-domain1] control-vlan 4092

# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceE-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device E as the master node of subring 2, with GigabitEthernet 1/0/1 as the primary
port and GigabitEthernet 1/0/2 as the secondary port. Enable subring 2.
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1
[DeviceE-rrpp-domain1] ring 2 enable
[DeviceE-rrpp-domain1] quit

# Enable RRPP.
[DeviceE] rrpp enable

6. Configure Device F:

# Create VLANs 1 through 30.
<DeviceF> system-view
[DeviceF] vlan 1 to 30

# Map these VLANs to MSTI 1.
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 1 to 30

# Activate the MST region configuration.
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceF-GigabitEthernet1/0/1] undo stp enable
# Configure the port as a trunk port.
[DeviceF-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 1 through 30.
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceF-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] link-delay 0
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[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.
[DeviceF] rrpp domain 1

# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceF-rrpp-domain1] control-vlan 4092

# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceF-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device F as the master node of subring 3, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable subring 3.
[DeviceF-rrpp-domain1] ring 3 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1
[DeviceF-rrpp-domain1] ring 3 enable
[DeviceF-rrpp-domain1] quit

# Enable RRPP.
[DeviceF] rrpp enable

7. Configure Device G:

# Create VLANs 1 through 30.
<DeviceG> system-view
[DeviceG] vlan 1 to 30

# Map these VLANs to MSTI 1.
[DeviceG] stp region-configuration
[DeviceG-mst-region] instance 1 vlan 1 to 30

# Activate the MST region configuration.
[DeviceG-mst-region] active region-configuration
[DeviceG-mst-region] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceG] interface gigabitethernet 1/0/1
[DeviceG-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceG-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceG-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 1 through 30.
[DeviceG-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceG-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceG] interface gigabitethernet 1/0/2
[DeviceG-GigabitEthernet1/0/2] link-delay 0
[DeviceG-GigabitEthernet1/0/2] undo stp enable
[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.
[DeviceG] rrpp domain 1

# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceG-rrpp-domain1] control-vlan 4092

# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceG-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device G as the master node of subring 4, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable subring 4.
[DeviceG-rrpp-domain1] ring 4 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1
[DeviceG-rrpp-domain1] ring 4 enable
[DeviceG-rrpp-domain1] quit

# Enable RRPP.
[DeviceG] rrpp enable

8. Configure Device H:

# Create VLANs 1 through 30.
<DeviceH> system-view
[DeviceH] vlan 1 to 30

# Map these VLANs to MSTI 1.
[DeviceH] stp region-configuration
[DeviceH-mst-region] instance 1 vlan 1 to 30

# Activate the MST region configuration.
[DeviceH-mst-region] active region-configuration
[DeviceH-mst-region] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceH] interface gigabitethernet 1/0/1
[DeviceH-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceH-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceH-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 1 through 30.
[DeviceH-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceH-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceH] interface gigabitethernet 1/0/2
[DeviceH-GigabitEthernet1/0/2] link-delay 0
[DeviceH-GigabitEthernet1/0/2] undo stp enable
[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.
[DeviceH] rrpp domain 1

# Configure VLAN 4092 as the primary control VLAN of RRPP domain 1.
[DeviceH-rrpp-domain1] control-vlan 4092

# Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.
[DeviceH-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device H as the master node of subring 5, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable subring 5.
[DeviceH-rrpp-domain1] ring 5 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1
[DeviceH-rrpp-domain1] ring 5 enable
[DeviceH-rrpp-domain1] quit

# Enable RRPP.
[DeviceH] rrpp enable

Verifying the configuration

# Use the display commands to view RRPP configuration and operational information on each device.

Load-balanced intersecting-ring configuration example

Network requirements

As shown in Figure 23:

- Device A, Device B, Device C, Device D, and Device F form RRPP domain 1. 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. 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 11 as the protected VLAN of domain 1, and VLAN 12 the protected VLAN of domain 2. You can implement VLAN-based load balancing on Ring 1.

- Ring 2 and Ring 3 have the same edge node and assistant edge node, and the two subrings have the same SRPTs. You can add Ring 2 and Ring 3 to an RRPP ring group to reduce Edge-Hello traffic.
Figure 23 Network diagram

Configuration procedure

1. Configure Device A:
   # Create VLANs 11 and 12.
   <DeviceA> system-view
   [DeviceA] vlan 11 to 12
   # Map VLAN 11 to MSTI 1 and VLAN 12 to MSTI 2.
   [DeviceA] stp region-configuration
   [DeviceA-mst-region] instance 1 vlan 11
   [DeviceA-mst-region] instance 2 vlan 12
   # Activate the MST region configuration.
   [DeviceA-mst-region] active region-configuration
   [DeviceA-mst-region] quit
   # Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] link-delay 0
   # Disable the spanning tree feature on the port.
   [DeviceA-GigabitEthernet1/0/1] undo stp enable
   # Configure the port as a trunk port.
   [DeviceA-GigabitEthernet1/0/1] port link-type trunk
   # Remove the port from VLAN 1, and assign it to VLANs 11 and 12.
   [DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
   [DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 11 12
   # Configure VLAN 11 as the default VLAN.
   [DeviceA-GigabitEthernet1/0/1] port trunk pvid vlan 11
   [DeviceA-GigabitEthernet1/0/1] quit
   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 11 12
[DeviceA-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceA-GigabitEthernet1/0/2] quit

# Create RRPP domain 1.
[DeviceA] rrpp domain 1

# Configure VLAN 100 as the primary control VLAN of RRPP domain 1.
[DeviceA-rrpp-domain1] control-vlan 100

# Configure the VLAN mapped to MSTI 1 as the protected VLAN of RRPP domain 1.
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the
primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit

# Create RRPP domain 2.
[DeviceA] rrpp domain 2

# Configure VLAN 105 as the primary control VLAN of RRPP domain 2.
[DeviceA-rrpp-domain2] control-vlan 105

# Configure the VLAN mapped to MSTI 2 as the protected VLAN of RRPP domain 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. 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 11 and 12.
<DeviceB> system-view
[DeviceB] vlan 11 to 12

# Map VLAN 11 to MSTI 1 and VLAN 12 to MSTI 2.
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 11
[DeviceB-mst-region] instance 2 vlan 12

# Activate the MST region configuration.
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceB-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceB-GigabitEthernet1/0/1] port link-type trunk

# Remove the port from VLAN 1, and assign it to VLANs 11 and 12.
[DeviceB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 11 12

# Configure VLAN 11 as the default VLAN.
[DeviceB-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceB-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 11 12
[DeviceB-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceB-GigabitEthernet1/0/2] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/3.
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceB-GigabitEthernet1/0/3] undo stp enable

# Configure the port as a trunk port.
[DeviceB-GigabitEthernet1/0/3] port link-type trunk

# Remove the port from VLAN 1, and assign it to VLAN 12.
[DeviceB-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 12

# Configure VLAN 12 as the default VLAN.
[DeviceB-GigabitEthernet1/0/3] port trunk pvid vlan 12
[DeviceB-GigabitEthernet1/0/3] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/4.
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceB-GigabitEthernet1/0/4] undo stp enable

# Configure the port as a trunk port.
[DeviceB-GigabitEthernet1/0/4] port link-type trunk

# Remove the port from VLAN 1, and assign it to VLAN 11.
[DeviceB-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 11

# Configure VLAN 11 as the default VLAN.
[DeviceB-GigabitEthernet1/0/4] port trunk pvid vlan 11
[DeviceB-GigabitEthernet1/0/4] quit

# Create RRPP domain 1.
[DeviceB] rrpp domain 1

# Configure VLAN 100 as the primary control VLAN of RRPP domain 1.
# Configure Device B as a transit node of primary ring 1 in RRPP domain 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

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

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

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

# Create RRPP domain 2.

```
[DeviceB] rrpp domain 2
```

# Configure VLAN 105 as the primary control VLAN of RRPP domain 2.

```
[DeviceB-rrpp-domain2] control-vlan 105
```

# Configure the VLAN mapped to MSTI 2 as the protected VLAN of RRPP domain 2.

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

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

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

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

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

# Enable RRPP.

```
[DeviceB] rrpp enable
```

3. Configure Device C:

# Create VLANs 11 and 12.

```
<DeviceC> system-view
[DeviceC] vlan 11 to 12
```

# Map VLAN 11 to MSTI 1 and VLAN 12 to MSTI 2.

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 11
[DeviceC-mst-region] instance 2 vlan 12
```

# Activate the MST region configuration.

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] link-delay 0
```
# Disable the spanning tree feature on the port.
[DeviceC-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceC-GigabitEthernet1/0/1] port link-type trunk

# Remove the port from VLAN 1, and assign it to VLANs 11 and 12.
[DeviceC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 11 12

# Configure VLAN 11 as the default VLAN.
[DeviceC-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceC-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] link-delay 0
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 11 12
[DeviceC-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceC-GigabitEthernet1/0/2] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/3.
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceC-GigabitEthernet1/0/3] undo stp enable

# Configure the port as a trunk port.
[DeviceC-GigabitEthernet1/0/3] port link-type trunk

# Remove the port from VLAN 1, and assign it to VLAN 12.
[DeviceC-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 12

# Configure VLAN 12 as the default VLAN.
[DeviceC-GigabitEthernet1/0/3] port trunk pvid vlan 12
[DeviceC-GigabitEthernet1/0/3] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/4.
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceC-GigabitEthernet1/0/4] undo stp enable

# Configure the port as a trunk port.
[DeviceC-GigabitEthernet1/0/4] port link-type trunk

# Remove the port from VLAN 1, and assign it to VLAN 11.
[DeviceC-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/4] port trunk permit vlan 11

# Configure VLAN 11 as the default VLAN.
[DeviceC-GigabitEthernet1/0/4] port trunk pvid vlan 11
[DeviceC-GigabitEthernet1/0/4] quit

# Create RRPP domain 1.
[DeviceC] rrpp domain 1
# Configure VLAN 100 as the primary control VLAN of RRPP domain 1.
[DeviceC-rrpp-domain1] control-vlan 100

# Configure the VLAN mapped to MSTI 1 as the protected VLAN of RRPP domain 1.
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device C as the transit node of primary ring 1 in RRPP domain 1, with
GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.
Enable ring 1.
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable

# Configure Device C as the edge node of subring 3 in RRPP domain 1, with GigabitEthernet
1/0/4 as the edge port. Enable subring 3.
[DeviceC-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceC-rrpp-domain1] ring 3 enable

# Create RRPP domain 2.
[DeviceC] rrpp domain 2

# Configure VLAN 105 as the primary control VLAN of RRPP domain 2.
[DeviceC-rrpp-domain2] control-vlan 105

# Configure the VLAN mapped to MSTI 2 as the protected VLAN of RRPP domain 2.
[DeviceC-rrpp-domain2] protected-vlan reference-instance 2

# Configure Device C as the transit node of primary ring 1 in RRPP domain 2, with
GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.
Enable ring 1.
[DeviceC-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain2] ring 1 enable

# Configure Device C as the edge node of subring 2 in RRPP domain 2, with GigabitEthernet
1/0/3 as the edge port. Enable subring 2.
[DeviceC-rrpp-domain2] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain2] ring 2 enable

# Enable RRPP.
[DeviceC] rrpp enable

4. Configure Device D:

# Create VLANs 11 and 12.
<DeviceD> system-view
[DeviceD] vlan 11 to 12

# Map VLAN 11 to MSTI 1 and VLAN 12 to MSTI 2.
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 11
[DeviceD-mst-region] instance 2 vlan 12

# Activate the MST region configuration.
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] link-delay 0
# Disable the spanning tree feature on the port.
[DeviceD-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceD-GigabitEthernet1/0/1] port link-type trunk

# Remove the port from VLAN 1, and assign it to VLANs 11 and 12.
[DeviceD-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 11 12

# Configure VLAN 11 as the default VLAN.
[DeviceD-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceD-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] link-delay 0
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 11 12
[DeviceD-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceD-GigabitEthernet1/0/2] quit

# Create RRPP domain 1.
[DeviceD] rrpp domain 1

# Configure VLAN 100 as the primary control VLAN of RRPP domain 1.
[DeviceD-rrpp-domain1] control-vlan 100

# Configure the VLAN mapped to MSTI 1 as the protected VLAN of RRPP domain 1.
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1

# Configure Device D as the transit node of primary ring 1 in RRPP domain 1, with
GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.
Enable ring 1.
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
[DeviceD-rrpp-domain1] quit

# Create RRPP domain 2.
[DeviceD] rrpp domain 2

# Configure VLAN 105 as the primary control VLAN of RRPP domain 2.
[DeviceD-rrpp-domain2] control-vlan 105

# Configure the VLAN mapped to MSTI 2 as the protected VLAN of RRPP domain 2.

# Configure Device D as the transit node of primary ring 1 in RRPP domain 2, with
GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.
Enable ring 1.
[DeviceD-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain2] ring 1 enable
[DeviceD-rrpp-domain2] quit

# Enable RRPP.
[DeviceD] rrpp enable

5. Configure Device E:
# Create VLAN 12.
[DeviceE] system-view
[DeviceE] vlan 12

# Map VLAN 12 to MSTI 2.
[DeviceE-vlan12] quit
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 2 vlan 12

# Activate the MST region configuration.
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceE-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceE-GigabitEthernet1/0/1] port link-type trunk

# Remove the port from VLAN 1, and assign it to VLAN 12.
[DeviceE-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 12

# Configure VLAN 12 as the default VLAN.
[DeviceE-GigabitEthernet1/0/1] port trunk pvid vlan 12
[DeviceE-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] link-delay 0
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 12
[DeviceE-GigabitEthernet1/0/2] port trunk pvid vlan 12
[DeviceE-GigabitEthernet1/0/2] quit

# Create RRPP domain 2.
[DeviceE] rrpp domain 2

# Configure VLAN 105 as the primary control VLAN of RRPP domain 2.
[DeviceE-rrpp-domain2] control-vlan 105

# Configure the VLAN mapped to MSTI 2 as the protected VLAN of RRPP domain 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. 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 11.

```
DeviceF> system-view
[DeviceF] vlan 11
[DeviceF-vlan11] quit
```

# Map VLAN 11 to MSTI 1.

```
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 11
```

# Activate the MST region configuration.

```
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit
```

# Set the physical state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] link-delay 0
```

# Disable the spanning tree feature on the port.

```
[DeviceF-GigabitEthernet1/0/1] undo stp enable
```

# Configure the port as a trunk port.

```
[DeviceF-GigabitEthernet1/0/1] port link-type trunk
```

# Remove the port from VLAN 1, and assign it to VLAN 11.

```
[DeviceF-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 11
```

# Configure VLAN 11 as the default VLAN.

```
[DeviceF-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceF-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] link-delay 0
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 11
[DeviceF-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceF-GigabitEthernet1/0/2] quit
```

# Create RRPP domain 1.

```
[DeviceF] rrpp domain 1
```

# Configure VLAN 100 as the primary control VLAN of RRPP domain 1.

```
[DeviceF-rrpp-domain1] control-vlan 100
```

# Configure the VLAN mapped to MSTI 1 as the protected VLAN of RRPP domain 1.

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

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

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

# Enable RRPP.

```
[DeviceF] rrpp enable
```

7. Configure RRPP ring group settings on Device B and Device C:
# Create RRPP ring group 1 on Device B, and 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
```

Verifying the configuration

```
# Use the display commands to view RRPP configuration and operational information on each device.
```

## Troubleshooting RRPP

### Symptom

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

### Solution

To resolve the problem:

1. Use the `display rrpp brief` command to determine 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.
2. Use the `display rrpp brief` command to determine 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.
3. Use the `display rrpp verbose` command to examine the link state of each port in each ring.
4. Use the `debugging rrpp` command on each node to determine whether a port receives or transmits Hello packets. If it does not, Hello packets are lost.
5. If the problem persists, contact Hewlett Packard Enterprise Support.
Configuring ERPS

Overview

Ethernet Ring Protection Switching (ERPS) is a robust link layer protocol that ensures a loop-free topology and implements quick link recovery.

ERPS structure

**Figure 24** ERPS ring structure

**Rings**

ERPS rings can be divided into major rings and subrings. An ERPS network consists of one major ring or multiple major rings, and multiple subrings. By default, a ring is a major ring. You can configure a ring as a subring manually.

As shown in **Figure 24**, a major ring is a closed ring formed by Device A, Device B, Device C, and Device D. A subring is an open ring formed by the link Device C<-->Device E<-->Device F<-->Device D.

**Nodes**

ERPS nodes include owner nodes, neighbor nodes, interconnection nodes, and normal nodes.

- The owner node and neighbor node block and unblock ports on the ring protection link (RPL) to prevent loops and switch traffic. An RPL connects an owner node and a neighbor node.
- Interconnection nodes connect different rings. Interconnection nodes reside on subrings and forward service packets but not protocol packets.
- Normal nodes forward both service packets and protocol packets.

As shown in **Figure 24**, on the major ring, Device A is the owner node and Device B is the neighbor node. On the subring, Device E is the owner node and Device F is the neighbor node. Devices C and D are interconnection nodes.

**Ports**

Each node consists of two ERPS ring member ports: Port 0 and port 1. ERPS ring member ports have the following types:
• **RPL port**—Port on an RPL link.
• **Interconnection port**—Port that connects a subring to a major ring.
• **Normal port**—Default type of a port that forwards both service packets and protocol packets.

As shown in Figure 24, ports A1, B1, E1, and F1 are RPL ports. Ports C3 and D3 are interconnection ports. Other ports are normal ports.

**Instances**

An ERPS ring supports multiple ERPS instances. An ERPS instance is a logical ring to process service and protocol packets. Each ERPS instance has its own owner node and maintains its own state and data. An ERPS instance is uniquely identified by the ring ID and VLAN ID of ERPS packets. The ring ID indicates the ring of ERPS packets. It can be represented by the last byte in the destination MAC address of the packets. The VLAN ID indicates the ERPS instance of the packets.

**ERPS protocol packets**

ERPS protocol packets are Ring Automatic Protection Switching (R-APS) packets. You can configure the R-APS packet level. A node does not process R-APS packets whose levels are greater than the level of the packets sent by the node. On a ring, the levels of R-APS packets must be the same for all nodes in an ERPS instance.

**Table 14 R-APS packet types and functions**

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>No request, RPL block (NR-RB)</td>
<td>When the link is stable, an owner node in idle state periodically sends NR-RB packets to inform other nodes that the RPL ports are blocked. The nodes that receive the NR-RB packets unblock available ports and update MAC address entries.</td>
</tr>
<tr>
<td>No request (NR)</td>
<td>After the link fault is cleared, the node that detects the recovery periodically sends NR packets. When the owner node receives the NR packets, it starts the WTR timer. The node stops sending NR packets after receiving NR-RB packets from the owner node.</td>
</tr>
<tr>
<td>Signal fail (SF)</td>
<td>When a link fails to send or receive signals, the node that detects the fault periodically sends SF packets. When the owner node and neighbor node receive the FS packets, they unblock the RPL ports. The node stops sending SF packets after the fault is cleared.</td>
</tr>
<tr>
<td>Manual switch (MS)</td>
<td>A port configured with the MS mode is blocked and periodically sends MS packets. When other nodes receive the MS packets, they unblock available ports and update MAC address entries.</td>
</tr>
<tr>
<td>Forced switch (FS)</td>
<td>A port configured with the FS mode is blocked and periodically sends FS packets. When other nodes receive the FS packets, they unblock all ports and update MAC address entries.</td>
</tr>
<tr>
<td>Flush</td>
<td>If the topology of a subring changes, the interconnection ports on the subring broadcasts flush packets. All nodes that receive the flush packets update MAC address entries.</td>
</tr>
</tbody>
</table>

**NOTE:**

- Typically R-APS packets are transmitted within a ring. The flush packets sourced from the subring can be forwarded to the major ring.
- Service packets can be transmitted between different rings.
ERPS node states

Table 15 ERPS states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Init</td>
<td>State for a non-interconnection node that has less than two ERPS ring member ports or for an interconnection node that does not have ERPS ring member ports.</td>
</tr>
<tr>
<td>Idle</td>
<td>Stable state when all non-RPL links are available. In this state, the owner node blocks the RPL port and periodically sends NR-RB packets. The neighbor node blocks the RPL port. All nodes enter the idle state after the owner node enters the idle state.</td>
</tr>
<tr>
<td>Protection</td>
<td>State when a non-RPL link is faulty. In this state, the RPL link is unblocked to forward traffic. All nodes enter the protection state after a node enters the protection state.</td>
</tr>
<tr>
<td>MS</td>
<td>State when traffic paths are manually switched. All nodes enter the MS state after a node is configured with the MS mode.</td>
</tr>
<tr>
<td>FS</td>
<td>State when traffic paths are forcibly switched. All nodes enter the FS state after a node is configured with the FS mode.</td>
</tr>
<tr>
<td>Pending</td>
<td>Transient state between the previous states.</td>
</tr>
</tbody>
</table>

ERPS timers

Table 16 ERPS timers

<table>
<thead>
<tr>
<th>Timer</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold-off</td>
<td>The hold-off timer starts when the port detects a link fault. The port reports the link fault if the fault persists when the timer expires.</td>
<td>This timer delays the fault report time and affects the link switching performance.</td>
</tr>
<tr>
<td>Guard</td>
<td>The guard timer starts when the port detects a link recovery. The port does not process R-APS packets before the timer expires.</td>
<td>This timer prevents R-APS packets from impacting the network and affects the link switching performance when multiple points of failures exist.</td>
</tr>
<tr>
<td>WTR</td>
<td>In revertive mode, the WTR timer starts when the owner node in protection state receives NR packets. The RPL is unblocked and the recovered node is blocked before the timer expires. The owner node blocks the RPL and sends NR-RB packets when the timer expires. If the port receives SF packets before the timer expires, the timer stops and the RPL remains unblocked.</td>
<td>This timer prevents intermittent link failures from impacting the network.</td>
</tr>
<tr>
<td>WTB</td>
<td>In revertive mode, the WTB timer starts when the owner node in MS or FS state receives NR packets. The RPL is unblocked and the recovered node sends NR packets before the timer expires. The owner node blocks the RPL and sends NR-RB packets when the timer expires. If the port receives SF packets before the timer expires, the timer stops and the RPL remains unblocked.</td>
<td>This timer prevents the RPL ports from being blocked and unblocked frequently.</td>
</tr>
</tbody>
</table>
ERPS operation mechanism

ERPS uses the detection mechanism defined in ITU-T G.8032/Y.1344 to locate the point of failure and identify unidirectional or bidirectional faults.

ERPS uses the SF packets to report signal failures on a link and the NR packets to report link recovery. When a node detects a link status change, the node sends three packets first and then sends subsequent packets every five seconds.

Link-down report mechanism

**Figure 25 Link-down report mechanism**

As shown in Figure 25, the link-down report mechanism uses the following process:
1. Device C and Device D detect the link failure and perform the following operations:
   a. Block the ports on both side of the faulty link.
   b. Periodically send SF packets to other nodes.
2. Device A and Device B receive the SF packets and perform the following operations:
   a. Unblock RPL ports.
   b. Update the MAC address entries.

Service packets are switched to the RPL link.

Link recovery mechanism

**Figure 26 Link recovery mechanism**

As shown in Figure 26, the link recovery mechanism uses the following process:
1. Device C and Device D detect the link recovery and perform the following operations:
   a. Block the recovered ports.
   b. Start the guard timer.
   c. Send NR packets.
2. When Device A (owner node) receives the NR packets, it does not perform any operations if it is in non-revertive mode. If Device A is in revertive mode, it performs the following operations:
a. Starts the WTR timer.
b. Blocks the RPL port and periodically sends NR-RB packets when the WTR timer expires.

3. When other nodes receive the NR-RB packets, they perform the following operations:
   a. Device B (neighbor port) blocks the RPL port.
   b. Device C and Device D unblock the recovered ports.

Service packets are switched to the recovered link.

**Multi-instance load balancing mechanism**

![Multi-instance load balancing mechanism](image)

An ERPS ring topology might carry traffic from multiple VLANs. Traffic from different VLANs can be load balanced among different ERPS instances.

ERPS uses the following types of VLANs:

- **Control VLAN**—Carries ERPS protocol packets. The system determines the control VLANs for ERPS ring member ports. Each ERPS instance has its own control VLAN.
- **Protected VLAN**—Carries data packets. Each ERPS instance has its own protected VLAN. Protected VLANs are configured by using the mappings between VLANs and MSTIs.

As shown in Figure 27, the ERPS ring is configured with instance 1 and instance 2. For instance 1, the owner node is Device A, and the RPL is the link between Device A and Device B. For instance 2, the owner node is Device C, and the RPL is the link between Device C and Device D. Traffic from different VLANs can be load balanced among different links.

**Manual configuration mechanism**

ERPS supports the following manual configuration modes:

- **MS**—Use the `erps switch manual` command to block an ERPS ring member port. A port in MS mode is blocked and sends MS packets. The nodes that receive the MS packets unblock available ports. If the nodes in MS mode receive an SF packet, they unblock the blocked ports.
- **FS**—Use the `erps switch force ring` command to block an ERPS ring member port. A port in FS mode is blocked and sends FS packets. The nodes that receive the FS packets unblock available ports. If the nodes in FS mode receive an SF packet, they do not unblock the blocked ports.

**Collaboration mechanism**

To detect and clear link faults typically for a fiber link, use ERPS with CFD and Track. You can associate ERPS ring member ports with the continuity check function of CFD through track entries. CFD reports link events only when the monitored VLAN is the control VLAN of the ERPS instance for the port. For more information about CFD and Track, see "Configuring CFD" and "Configuring Track."
ERPS network diagrams

One major ring
The network has one major ring.

Figure 28 Network diagram

One major ring connecting one subring
The network has one major ring and one subring.

Figure 29 Network diagram

One major ring connecting multiple subrings
The network has three or more rings. Each subring is connected to the major ring by two interconnection nodes.
One subring connecting multiple subrings

The network has three or more rings. As shown in Figure 31, subring 1 is connected to the major ring. Other subrings are connected to subring 1 by two interconnection nodes.

Figure 31 Network diagram

One subring connecting multiple rings

The network has three or more rings. A minimum of one subring is connected to two rings. As shown in Figure 32, one interconnection node on subring 2 is connected to the major ring; and another interconnection node is connected to subring 1. As shown in Figure 33, subring 3 is connected to subring 1 and subring 2.
Protocols and standards

- IEEE 802.1D, IEEE Std 802.1D™-2004, IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Bridges
- IEEE 802.3, IEEE Std 802.3-2008, IEEE Standard for Information technology

ERPS configuration task list

ERPS does not provide an election mechanism. To implement ring detection and protection, configure all nodes correctly.

To configure ERPS, perform the following tasks:
Task at a glance | Remarks
--- | ---
(Required.) Enabling ERPS globally | N/A
(Required.) Enabling flush packet transparent transmission | N/A
(Required.) Configuring an ERPS ring | N/A
(Optional.) Enabling R-APS packets to carry the ring ID in the destination MAC address | N/A
(Required.) Configuring ERPS ring member ports:  
- Configuring ERPS ring member port attributes  
- Configuring an ERPS ring member port | N/A
(Required.) Configuring control VLANs | N/A
(Required.) Configuring protected VLANs | N/A
(Required.) Configuring the node role | N/A
(Required.) Enabling ERPS for an instance | N/A
(Optional.) Configuring R-APS packet levels | N/A
(Optional.) Setting ERPS timers | This task is required only for the owner node.
(Optional.) Setting the non-revertive mode | This task is required only for the owner node.
(Optional.) Setting the MS mode | This task is required for the node whose port is blocked.
(Optional.) Setting the FS mode | This task is required for the node whose port is blocked.
(Optional.) Associating a ring with a subring | This task is required only for the interconnection node.
(Optional.) Associating an ERPS ring member port with a track entry | N/A
(Optional.) Removing the MS mode and FS mode settings for an ERPS ring | N/A

Configuration prerequisites

Before you configure ERPS, complete the following tasks:
- Establish the Ethernet ring topology.
- Determine the ERPS rings, ERPS instances, control VLANs, protected VLANs, and node roles.

Enabling ERPS globally

For ERPS to take effect for an instance, enable it globally first.

To enable ERPS globally:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable ERPS globally.</td>
<td>erps enable</td>
</tr>
</tbody>
</table>
Enabling flush packet transparent transmission

This feature enables the interconnection nodes to forward flush packets for topology changes in the subring to the major ring.

To enable flush packet transparent transmission:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enable flush packet</td>
<td>erps tcn-propagation By default, flush packet transparent</td>
</tr>
<tr>
<td></td>
<td>transparent transmission.</td>
<td>transparent transmission is disabled.</td>
</tr>
</tbody>
</table>

Configuring an ERPS ring

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Create an ERPS ring.</td>
<td>erps ring ring-id A ring ID uniquely identifies an ERPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ring. All nodes on an ERPS ring must be configured with the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>same ring ID.</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Configure the</td>
<td>ring-type sub-ring By default, an ERPS ring is a major ring.</td>
</tr>
<tr>
<td></td>
<td>ring type.</td>
<td></td>
</tr>
</tbody>
</table>

Enabling R-APS packets to carry the ring ID in the destination MAC address

Perform this task to configure the ring ID as the last byte of the destination MAC address for R-APS packets. The ring of R-APS packets can be identified by their destination MAC addresses.

To enable R-APS packets to carry the ring ID in the destination MAC address:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter ERPS ring view.</td>
<td>erps ring ring-id N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Enable R-APS packets to</td>
<td>r-aps ring-mac By default, R-APS packets do not carry ring</td>
</tr>
<tr>
<td></td>
<td>carry the ring ID in the</td>
<td>IDs in their destination MAC addresses. The last byte of the</td>
</tr>
<tr>
<td></td>
<td>destination MAC address.</td>
<td>destination MAC address is 1.</td>
</tr>
</tbody>
</table>

Configuring ERPS ring member ports

You can configure the ERPS ring member ports before configuring ERPS instances.
Configuring ERPS ring member port attributes

Follow these guidelines when you configure ERPS ring member port attributes:

- ERPS ring member ports automatically allow packets from the control VLAN to pass through.
- Do not enable Ethernet OAM remote loopback for ERPS ring member ports. This feature might cause a broadcast storm. For more information about Ethernet OAM, see "Configuring Ethernet OAM."
- For faster topology convergence, use the `link-delay` command on ERPS ring member ports to set the physical state change suppression interval to 0 seconds. For more information about the `link-delay` command, see Interface Command Reference.
- You must configure ERPS ring member ports as trunk ports.

To configure ERPS ring member port attributes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the port as a trunk port.</td>
<td>port link-type trunk</td>
</tr>
<tr>
<td>4.</td>
<td>Assign the trunk port to protected VLANs.</td>
<td>port trunk permit vlan { vlan-id-list</td>
</tr>
<tr>
<td>5.</td>
<td>Disable the spanning tree feature.</td>
<td>undo stp enable</td>
</tr>
</tbody>
</table>

Configuring an ERPS ring member port

Only trunk ports can be configured as the ERPS ring member ports.

To configure an ERPS ring member port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter ERPS ring view.</td>
<td>erps ring ring-id</td>
</tr>
<tr>
<td>3.</td>
<td>Configure an ERPS ring member port.</td>
<td>{ port0</td>
</tr>
</tbody>
</table>

By default, an ERPS ring does not have ERPS ring member ports.
Configuring control VLANs

Follow these guidelines when you configure control VLANs:

- Configure the same control VLAN for all nodes in an ERPS instance.
- Do not configure the default VLAN of an ERPS ring member port as the control VLAN, and do not enable QinQ or VLAN mapping on control VLANs. If you do, ERPS packets cannot be correctly forwarded and received.
- Make sure the ERPS instance has been configured. After the ERPS instance is enabled, the control VLAN cannot be changed.
- For a device that connects two rings to forward Flush packets correctly, make sure only the ports that connect to the ERPS rings are configured with the control VLAN.
- For a device not configured with ERPS to transparently transmit ERPS packets, make sure only the two ports accessing the ERPS ring permit packets from the control VLAN. If other ports on the device permit packets from the control VLAN, the packets from other VLANs might enter the control VLAN and strike the ERPS ring.

To configure a control VLAN:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter ERPS ring view.</td>
<td>erps ring ring-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enable ERPS instance view.</td>
<td>instance instance-id</td>
</tr>
<tr>
<td>4.</td>
<td>Configure a control VLAN.</td>
<td>control-vlan vlan-id</td>
</tr>
</tbody>
</table>

Configuring protected VLANs

Configure the same protected VLAN for all nodes of an ERPS instance. To implement load balancing, configure different protected VLANs for different ERPS instances.

Protected VLANs are configured by referencing MSTIs. The protected VLAN configuration method varies by the spanning tree mode:

- In STP, RSTP, or MSTP mode, you must manually configure the mappings between VLANs and MSTIs.
- In PVST mode, the device automatically maps each VLAN to an MSTI. When the spanning tree protocol is disabled globally, all VLANs are automatically mapped to MSTI 0.

For more information about MSTI and PVST, see *Layer 2—LAN Switching Configuration Guide*. To configure protected VLANs:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter MST region view.</td>
<td>stp region-configuration</td>
</tr>
</tbody>
</table>
3. Map VLANs to MSTIs.
   - Method 1: `instance instance-id vlan vlan-list`
   - Method 2: `vlan-mapping modulo modulo`
   By default, all VLANs are mapped to MSTI 0 (CIST).
   This step is not required if the device is operating in PVST mode.
   For more information about these commands, see Layer 2—LAN Switching Command Reference.

4. Activate the MST region configuration.
   `active region-configuration`
   This step is not required if the device is operating in PVST mode.
   For more information about this command, see Layer 2—LAN Switching Command Reference.

5. (Optional.) Display the mapping between VLANs and MSTIs.
   `display stp region-configuration`
   Available in any view.
   The output of the command includes VLAN-to-instance mappings.
   For more information about this command, see Layer 2—LAN Switching Command Reference.

6. Return to system view.
   `quit`
   This step is not required if the device is operating in PVST mode.

7. Enter ERPS ring view.
   `erps ring ring-id`
   N/A

8. Enable ERPS instance view.
   `instance instance-id`
   N/A

9. Configure the protected VLANs.
   `protected-vlan reference-instance instance-id-list`
   By default, an ERPS instance does not have protected VLANs.

---

### Configuring the node role

You can only configure the interconnection node for subrings.

To configure the node role:

1. Enter system view.
   `system-view`
   N/A

2. Enter ERPS ring view.
   `erps ring ring-id`
   N/A

3. Enter ERPS instance view.
   `instance instance-id`
   N/A

4. Configure the node role.
   `node-role { { owner | neighbor } rpl | interconnection } { port0 | port1 }
   By default, a node is a normal node.

---

### Enabling ERPS for an instance

You can enable ERPS for an instance only when it is configured with a control VLAN and a protected VLAN.

To enable ERPS for an instance:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter ERPS ring view.</td>
<td>erps ring ring-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enter ERPS instance view.</td>
<td>instance instance-id</td>
</tr>
<tr>
<td>4.</td>
<td>Enable ERPS for the instance.</td>
<td>instance enable</td>
</tr>
</tbody>
</table>

### Configuring R-APS packet levels

A node does not process R-APS packets whose levels are greater than the level of R-APS packets sent by the node. On a ring, the levels of R-APS packets must be the same for all nodes in an ERPS instance.

To configure the R-APS packet level:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter ERPS ring view.</td>
<td>erps ring ring-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enter ERPS instance view.</td>
<td>instance instance-id</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the R-APS packet level.</td>
<td>r-aps level level-value</td>
</tr>
</tbody>
</table>

### Setting ERPS timers

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter ERPS ring view.</td>
<td>erps ring ring-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enter ERPS instance view.</td>
<td>instance instance-id</td>
</tr>
<tr>
<td>4.</td>
<td>Set the guard timer.</td>
<td>timer guard guard-value</td>
</tr>
<tr>
<td>5.</td>
<td>Set the hold-off timer.</td>
<td>timer hold-off hold-off-value</td>
</tr>
<tr>
<td>6.</td>
<td>Set the WTR timer.</td>
<td>timer wtr wtr-value</td>
</tr>
</tbody>
</table>

### Setting the non-revertive mode

Set the non-revertive mode as required.

To set the non-revertive mode:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter ERPS ring view.</td>
<td>erps ring ring-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enter ERPS instance view.</td>
<td>instance instance-id</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the node as the owner node and port 0 as the RPL port.</td>
<td>node-role owner rpl port0</td>
</tr>
<tr>
<td>5.</td>
<td>Set the non-revertive mode.</td>
<td>revertive-operation non-revertive</td>
</tr>
</tbody>
</table>

**Setting the MS mode**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the MS mode.</td>
<td>erps switch manual ring ring-id instance instance-id { port0</td>
</tr>
</tbody>
</table>

**Setting the FS mode**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the FS mode.</td>
<td>erps switch force ring ring-id instance instance-id { port0</td>
</tr>
</tbody>
</table>

**Associating a ring with a subring**

On a multi-ring network, configure the associated rings for a subring on the interconnection node.

To associate a ring with a subring:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter ERPS ring view.</td>
<td>erps ring ring-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enter ERPS instance view.</td>
<td>instance instance-id</td>
</tr>
<tr>
<td>4.</td>
<td>Associate a ring with the subring.</td>
<td>sub-ring connect ring ring-id instance instance-id</td>
</tr>
</tbody>
</table>
Associating an ERPS ring member port with a track entry

Before you associate a port with a track entry, make sure the port has joined an ERPS instance.

To associate an ERPS ring member port with a track entry:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Associate an ERPS ring member port with a track entry.</td>
<td>port erps ring ring-id instance instance-id track track-entry-index</td>
</tr>
</tbody>
</table>

Removing the MS mode and FS mode settings for an ERPS ring

After you configure this task, the owner node can ignore the WTR timer and immediately switch traffic to the recovered link upon link recovery.

This task also switches an ERPS ring in non-revertive mode to revertive mode.

To remove the MS mode and FS mode settings for an ERPS ring:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Remove the MS mode and FS mode settings for an ERPS ring.</td>
<td>erps clear ring ring-id instance instance-id</td>
</tr>
</tbody>
</table>

Displaying and maintaining ERPS

Execute display commands in any view and reset commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display brief ERPS information.</td>
<td>display erps</td>
</tr>
<tr>
<td>Display detailed ERPS information.</td>
<td>display erps detail ring ring-id [ instance instance-id ]</td>
</tr>
<tr>
<td>Display ERPS packet statistics.</td>
<td>display erps statistics [ ring ring-id [ instance instance-id ] ]</td>
</tr>
<tr>
<td>Clear ERPS packet statistics.</td>
<td>reset erps statistics ring ring-id [ instance instance-id ]</td>
</tr>
</tbody>
</table>
ERPS configuration examples

One-ring configuration example

Network requirements

As shown in Figure 34, perform the following tasks to eliminate loops on the network:

- Configure the ring as ERPS ring 1.
- Configure VLAN 100 as the control VLAN for ERPS ring 1.
- Configure VLANs 1 to 30 as the protected VLANs for ERPS ring 1.
- Configure Device A as the owner node, GigabitEthernet 1/0/1 as ERPS ring member port 0 and the RPL port, and GigabitEthernet 1/0/2 as ERPS ring member port 1.
- Configure Device B as the neighbor node, GigabitEthernet 1/0/1 as ERPS ring member port 0 and the RPL port, and GigabitEthernet 1/0/2 as ERPS ring member port 1.
- Configure Device C and Device D as normal nodes, GigabitEthernet 1/0/1 as ERPS ring member port 0, and GigabitEthernet 1/0/2 as ERPS ring member port 1.

![Figure 34 Network diagram](Diagram)

Configuration procedure

1. Configure Device A.

   # Create VLANs 1 to 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
   # Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
   [DeviceA-GigabitEthernet1/0/1] link-delay 0
   # Disable the spanning tree feature on the port.
   [DeviceA-GigabitEthernet1/0/1] undo stp enable
   # Configure the port as a trunk port and assign it to VLANs 1 to 30.
   [DeviceA-GigabitEthernet1/0/1] port link-type trunk
   [DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
   [DeviceA-GigabitEthernet1/0/1] quit
   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
   ```
DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[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 ERPS ring 1.
[DeviceA] erps ring 1

# Configure ERPS ring member ports.
[DeviceA-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceA-erps-ring1] port1 interface gigabitethernet 1/0/2

# Enable R-APS packets to carry ring ID in the destination MAC address.
[DeviceA-erps-ring1] r-aps ring-mac

# Create ERPS instance 1.
[DeviceA-erps-ring1] instance 1

# Configure the node role.
[DeviceA-erps-ring1-inst1] node-role owner rpl port0

# Configure the control VLAN.
[DeviceA-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.
[DeviceA-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.
[DeviceA-erps-ring1-inst1] instance enable
[DeviceA-erps-ring1-inst1] quit

# Enable CFD, and create a level-5 MD named MD_A.
[DeviceA] cfd enable
[DeviceA] cfd md MD_A level 5

# Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.
[DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1

# Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1001 in Ethernet service instance 1, and enable CCM sending 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 1001 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable

# Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.
[DeviceA] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2

# Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2001 in Ethernet service instance 1, and enable CCM sending 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 2001 service-instance 2 outbound
[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceA-GigabitEthernet1/0/2] quit
# Create track entry 1 and associate it with the CC function of CFD for MEP 1001 in Ethernet service instance 1.

[DeviceA] track 1 cfd cc service-instance 1 mep 1001

# Associate GigabitEthernet 1/0/1 with track entry 1 and bring up the port.

[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 2001 in Ethernet service instance 2.

[DeviceA] track 2 cfd cc service-instance 2 mep 2001

# Associate GigabitEthernet 1/0/2 with track entry 2 and bring up the port.

[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
[DeviceA-GigabitEthernet1/0/2] quit

# Enable ERPS.

[DeviceA] erps enable

2. Configure Device B.

# Create VLANs 1 to 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

# Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.

[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] port link-type trunk

# Configure the port as a trunk port and assign it to VLANs 1 to 30.

[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[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 ERPS ring 1.

[DeviceB] erps ring 1

# Configure ERPS ring member ports.

[DeviceB-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceB-erps-ring1] port1 interface gigabitethernet 1/0/2
# Enable R-APS packets to carry ring ID in the destination MAC address.
[DeviceB-erps-ring1] r-aps ring-mac

# Create ERPS instance 1.
[DeviceB-erps-ring1] instance 1

# Configure the node role.
[DeviceB-erps-ring1-inst1] node-role neighbor rpl port0

# Configure the control VLAN.
[DeviceB-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.
[DeviceB-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.
[DeviceB-erps-ring1-inst1] instance enable
[DeviceB-erps-ring1-inst1] quit
[DeviceB-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD_A.
[DeviceB] cfd enable
[DeviceB] cfd md MD_A level 5

# Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.
[DeviceB] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1

# Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1002 in Ethernet service instance 1, and enable CCM sending on GigabitEthernet 1/0/1.
[DeviceB] cfd meplist 1001 1002 service-instance 1
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound
[DeviceB-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceB-GigabitEthernet1/0/1] quit

# Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.
[DeviceB] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3

# Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3002 in Ethernet service instance 1, and enable CCM sending on GigabitEthernet 1/0/2.
[DeviceB] cfd meplist 3001 3002 service-instance 3
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] cfd mep 3002 service-instance 3 outbound
[DeviceB-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3002 enable
[DeviceB-GigabitEthernet1/0/2] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 1002 in Ethernet service instance 1.
[DeviceB] track 1 cfd cc service-instance 1 mep 1002

# Associate GigabitEthernet 1/0/1 with track entry 1 and bring up the port.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceB-GigabitEthernet1/0/1] undo shutdown
[DeviceB-GigabitEthernet1/0/1] quit

# Create track entry 3 and associate it with the CC function of CFD for MEP 3002 in Ethernet service instance 3.
[DeviceB] track 3 cfd cc service-instance 3 mep 3002
# Associate GigabitEthernet 1/0/2 with track entry 3 and bring up the port.
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceB-GigabitEthernet1/0/2] undo shutdown
[DeviceB-GigabitEthernet1/0/2] quit
#
# Enable ERPS.
[DeviceB] erps enable

3. Configure Device C.
#
# Create VLANs 1 to 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
#
# Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] link-delay 0
#
# Disable the spanning tree feature on the port.
[DeviceC-GigabitEthernet1/0/1] undo stp enable
#
# Configure the port as a trunk port and assign it to VLANs 1 to 30.
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
#
# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] link-delay 0
[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 ERPS ring 1.
[DeviceC] erps ring 1
#
# Configure ERPS ring member ports.
[DeviceC-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceC-erps-ring1] port1 interface gigabitethernet 1/0/2
#
# Enable R-APS packets to carry ring ID in the destination MAC address.
[DeviceC-erps-ring1] r-aps ring-mac
#
# Create ERPS instance 1.
[DeviceC-erps-ring1] instance 1
#
# Configure the control VLAN.
[DeviceC-erps-ring1-inst1] control-vlan 100
#
# Configure the protected VLANs.
[DeviceC-erps-ring1-inst1] protected-vlan reference-instance 1
#
# Enable ERPS for instance 1.
[DeviceC-erps-ring1-inst1] instance enable
Configure Device C.

# Enable CFD, and create a level-5 MD named MD_A.

[DeviceC] cfd enable
[DeviceC] cfd md MD_A level 5

# Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.

[DeviceC] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3

# Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3001 in Ethernet service instance 3, and enable CCM sending on GigabitEthernet 1/0/1.

[DeviceC] cfd meplist 3001 3002 service-instance 3
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 3001 service-instance 3 outbound
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 3 mep 3001 enable

# Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.

[DeviceC] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4

# Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4001 in Ethernet service instance 4, and enable CCM sending on GigabitEthernet 1/0/2.

[DeviceC] cfd meplist 4001 4002 service-instance 4
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd mep 4001 service-instance 4 outbound
[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 4 mep 4001 enable

# Create track entry 1 and associate it with the CC function of CFD for MEP 3001 in Ethernet service instance 3.

[DeviceC] track 1 cfd cc service-instance 3 mep 3001

# Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port.

[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceC-GigabitEthernet1/0/2] undo shutdown

# Create track entry 2 and associate it with the CC function of CFD for MEP 4001 in Ethernet service instance 4.

[DeviceC] track 2 cfd cc service-instance 4 mep 4001

# Associate GigabitEthernet 1/0/1 with track entry 3 and bring up the port.

[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceC-GigabitEthernet1/0/1] undo shutdown

# Enable ERPS.

[DeviceC] erps enable

4. Configure Device D.

# Create VLANs 1 to 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

# Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceD-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 30.
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] link-delay 0
[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 ERPS ring 1.
[DeviceD] erps ring 1

# Configure ERPS ring member ports.
[DeviceD-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceD-erps-ring1] port1 interface gigabitethernet 1/0/2

# Enable R-APS packets to carry ring ID in the destination MAC address.
[DeviceD-erps-ring1] r-aps ring-mac

# Create ERPS instance 1.
[DeviceD-erps-ring1] instance 1

# Configure the control VLAN.
[DeviceD-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.
[DeviceD-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.
[DeviceD-erps-ring1-inst1] instance enable
[DeviceD-erps-ring1-inst1] quit

# Enable CFD, and create a level-5 MD named MD_A.
[DeviceD] cfd enable
[DeviceD] cfd md MD_A level 5

# Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.
[DeviceD] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2

# Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2002 in Ethernet service instance 2, and enable CCM sending on GigabitEthernet 1/0/2.
[DeviceD] cfd meplist 2001 2002 service-instance 2
[DeviceD] interface gigabitethernet 1/0/2
# Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.

```bash
[DeviceD] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4
```

# Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4002 in Ethernet service instance 4, and enable CCM sending on GigabitEthernet 1/0/1.

```bash
[DeviceD] cfd meplist 4001 4002 service-instance 4
```

```bash
[DeviceD-GigabitEthernet1/0/1] cfd mep 4002 service-instance 4 outbound
```

```bash
[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4002 enable
```

```bash
[DeviceD-GigabitEthernet1/0/1] quit
```

# Create track entry 1 and associate it with the CC function of CFD for MEP 2002 in Ethernet service instance 2.

```bash
[DeviceD] track 1 cfd cc service-instance 2 mep 2002
```

# Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port.

```bash
[DeviceD] interface gigabitethernet 1/0/2
```

```bash
[DeviceD-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
```

```bash
[DeviceD-GigabitEthernet1/0/2] undo shutdown
```

```bash
[DeviceD-GigabitEthernet1/0/2] quit
```

# Create track entry 2 and associate it with the CC function of CFD for MEP 4002 in Ethernet service instance 4.

```bash
[DeviceD] track 2 cfd cc service-instance 4 mep 4002
```

# Associate GigabitEthernet 1/0/1 with track entry 2 and bring up the port.

```bash
[DeviceD] interface gigabitethernet 1/0/1
```

```bash
[DeviceD-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
```

```bash
[DeviceD-GigabitEthernet1/0/1] undo shutdown
```

```bash
[DeviceD-GigabitEthernet1/0/1] quit
```

# Enable ERPS.

```bash
[DeviceD] erps enable
```

## Verifying the configuration

# Display information about ERPS instance 1 for Device A.

```bash
[DeviceA] display erps detail ring 1
```

<table>
<thead>
<tr>
<th>Ring ID</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port0</td>
<td>GigabitEthernet1/0/1</td>
</tr>
<tr>
<td>Port1</td>
<td>GigabitEthernet1/0/2</td>
</tr>
<tr>
<td>Subring</td>
<td>No</td>
</tr>
<tr>
<td>Default MAC</td>
<td>No</td>
</tr>
<tr>
<td>Instance ID</td>
<td>1</td>
</tr>
<tr>
<td>Node role</td>
<td>Owner</td>
</tr>
<tr>
<td>Node state</td>
<td>Idle</td>
</tr>
<tr>
<td>Connect</td>
<td>-</td>
</tr>
<tr>
<td>Control VLAN</td>
<td>100</td>
</tr>
<tr>
<td>Protected VLAN</td>
<td>Reference-instance 1</td>
</tr>
<tr>
<td>Guard timer</td>
<td>500 ms</td>
</tr>
<tr>
<td>Hold-off timer</td>
<td>0 ms</td>
</tr>
</tbody>
</table>
The output shows the following information:

- Device A is the owner node.
- The ERPS ring is in idle state.
- The RPL port is blocked.
- The non-RPL port is unblocked.

### One-subring configuration example

#### Network requirements

As shown in Figure 35, perform the following tasks to eliminate loops on the network:

- Configure VLAN 100 and VLAN 200 as the control VLANs for the major ring and the subring, respectively.
- Configure VLANs 1 to 30 as the protected VLANs for the major ring and subring.
- Configure Device A as the owner node for the major ring, GigabitEthernet 1/0/1 as ERPS ring member port 0 and the RPL port, and GigabitEthernet 1/0/2 as ERPS ring member port 1.
- Configure Device B as the neighbor node for the major ring, GigabitEthernet 1/0/1 as ERPS ring member port 0 and the RPL port, and GigabitEthernet 1/0/2 as ERPS ring member port 1.
- Configure Devices C and D as interconnection nodes, GigabitEthernet 1/0/1 as ERPS ring member port 0, GigabitEthernet 1/0/2 as ERPS ring member port 1, and GigabitEthernet 1/0/3 as the interconnection port.
- Configure Device E as the owner node for the subring, GigabitEthernet 1/0/1 as ERPS ring member port 0 and the RPL port, and GigabitEthernet 1/0/2 as ERPS ring member port 1.
- Configure Device F as the neighbor node for the subring, GigabitEthernet 1/0/1 as ERPS ring member port 0 and the RPL port, and GigabitEthernet 1/0/2 as ERPS ring member port 1.
Figure 35 Network diagram

Configuration procedure

1. Configure Device A.
   # Create VLANs 1 to 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
   # Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] link-delay 0
   # Disable the spanning tree feature on the port.
   [DeviceA-GigabitEthernet1/0/1] undo stp enable
   # Configure the port as a trunk port and assign it to VLANs 1 to 30.
   [DeviceA-GigabitEthernet1/0/1] port link-type trunk
   [DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
   [DeviceA-GigabitEthernet1/0/1] quit
   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] link-delay 0
   [DeviceA-GigabitEthernet1/0/2] undo stp enable
   [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 ERPS ring 1.
   [DeviceA] erps ring 1
   # Configure ERPS ring member ports.
   [DeviceA-erps-ring1] port0 interface gigabitethernet 1/0/1
   [DeviceA-erps-ring1] port1 interface gigabitethernet 1/0/2
# Create ERPS instance 1.
[DeviceA-erps-ring1] instance 1

# Configure the node role.
[DeviceA-erps-ring1-inst1] node-role owner rpl port0

# Configure the control VLAN.
[DeviceA-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.
[DeviceA-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.
[DeviceA-erps-ring1-inst1] instance enable
[DeviceA-erps-ring1-inst1] quit
[DeviceA-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD_A.
[DeviceA] cfd enable
[DeviceA] cfd md MD_A level 5

# Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.
[DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1

# Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1001 in Ethernet service instance 1, and enable CCM sending 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 1001 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] quit

# Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.
[DeviceA] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2

# Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2001 in Ethernet service instance 1, and enable CCM sending 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 2001 service-instance 2 outbound
[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceA-GigabitEthernet1/0/2] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 1001 in Ethernet service instance 1.
[DeviceA] track 1 cfd cc service-instance 1 mep 1001

# Associate GigabitEthernet 1/0/1 with track entry 1 and bring up the port.
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 2001 in Ethernet service instance 2.
[DeviceA] track 2 cfd cc service-instance 2 mep 2001

# Associate GigabitEthernet 1/0/2 with track entry 2 and bring up the port.
[DeviceA] interface gigabitethernet 1/0/2
1. Configure Device A.

   # Enable ERPS.
   [DeviceA] erps enable

   [DeviceA-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
   [DeviceA-GigabitEthernet1/0/2] undo shutdown
   [DeviceA-GigabitEthernet1/0/2] quit

2. Configure Device B.

   # Create VLANs 1 to 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

   # Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
   [DeviceB] interface gigabitethernet 1/0/1
   [DeviceB-GigabitEthernet1/0/1] link-delay 0

   # Disable the spanning tree feature on the port.
   [DeviceB-GigabitEthernet1/0/1] undo stp enable

   # Configure the port as a trunk port and assign it to VLANs 1 to 30.
   [DeviceB-GigabitEthernet1/0/1] port link-type trunk
   [DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
   [DeviceB-GigabitEthernet1/0/1] quit

   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
   [DeviceB] interface gigabitethernet 1/0/2
   [DeviceB-GigabitEthernet1/0/2] link-delay 0
   [DeviceB-GigabitEthernet1/0/2] undo stp enable
   [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 ERPS ring 1.
   [DeviceB] erps ring 1

   # Create ERPS ring member ports.
   [DeviceB-erps-ring1] port0 interface gigabitethernet 1/0/1
   [DeviceB-erps-ring1] port1 interface gigabitethernet 1/0/2

   # Create ERPS instance 1.
   [DeviceB-erps-ring1-inst1] instance 1

   # Configure the node role.
   [DeviceB-erps-ring1-inst1] node-role neighbor rpl port0

   # Configure the control VLAN.
   [DeviceB-erps-ring1-inst1] control-vlan 100

   # Configure the protected VLANs.
   [DeviceB-erps-ring1-inst1] protected-vlan reference-instance 1

   # Enable ERPS for instance 1.
   [DeviceB-erps-ring1-inst1] instance enable
   [DeviceB-erps-ring1-inst1] quit
   [DeviceB-erps-ring1] quit
# Enable CFD, and create a level-5 MD named MD_A.
[DeviceB] cfd enable
[DeviceB] cfd md MD_A level 5

# Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.
[DeviceB] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1

# Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1002 in Ethernet service instance 1, and enable CCM sending on GigabitEthernet 1/0/1.
[DeviceB] cfd meplist 1001 1002 service-instance 1
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound
[DeviceB-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceB-GigabitEthernet1/0/1] quit

# Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.
[DeviceB] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3

# Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3002 in Ethernet service instance 2, and enable CCM sending on GigabitEthernet 1/0/2.
[DeviceB] cfd meplist 3001 3002 service-instance 3
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] cfd mep 3002 service-instance 3 outbound
[DeviceB-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3002 enable
[DeviceB-GigabitEthernet1/0/2] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 1002 in Ethernet service instance 1.
[DeviceB] track 1 cfd cc service-instance 1 mep 1002

# Associate GigabitEthernet 1/0/1 with track entry 1 and bring up the port.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceB-GigabitEthernet1/0/1] undo shutdown
[DeviceB-GigabitEthernet1/0/1] quit

# Create track entry 3 and associate it with the CC function of CFD for MEP 3002 in Ethernet service instance 3.
[DeviceB] track 3 cfd cc service-instance 3 mep 3002

# Associate GigabitEthernet 1/0/2 with track entry 3 and bring up the port.
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceB-GigabitEthernet1/0/2] undo shutdown
[DeviceB-GigabitEthernet1/0/2] quit

# Enable ERPS.
[DeviceB] erps enable

3. Configure Device C.
# Create VLANs 1 to 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
Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

Enable the spanning tree feature on the port.

Configure the port as a trunk port and assign it to VLANs 1 to 30.

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.

Create ERPS ring 1.

Configure ERPS ring member ports.

Create ERPS ring member ports.

Create ERPS instance 1.

Configure the control VLAN.

Configure the protected VLANs.

Enable ERPS for instance 1.

Enable CFD, and create a level-5 MD named MD_A.

Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.

Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3001 in Ethernet service instance 3, and enable CCM sending on GigabitEthernet 1/0/2.
[DeviceC] cfd meplist 3001 3002 service-instance 3
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd mep 3001 service-instance 3 outbound
[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3001 enable
[DeviceC-GigabitEthernet1/0/2] quit

# Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.
[DeviceC] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4
# Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4001 in Ethernet service instance 4, and enable CCM sending on GigabitEthernet 1/0/1.
[DeviceC] cfd meplist 4001 4002 service-instance 4
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 4001 service-instance 4 outbound
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4001 enable
[DeviceC-GigabitEthernet1/0/1] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 3001 in Ethernet service instance 3.
[DeviceC] track 1 cfd cc service-instance 3 mep 3001
# Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port.
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 4001 in Ethernet service instance 4.
[DeviceC] track 2 cfd cc service-instance 4 mep 4001
# Associate GigabitEthernet 1/0/1 with track entry 2 and bring up the port.
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit

# Create ERPS ring 2.
[DeviceC] erps ring 2
# Configure ERPS ring member ports.
[DeviceC-erps-ring2] port0 interface gigabitethernet 1/0/3
# Configure ERPS ring 2 as the subring.
[DeviceC-erps-ring2] ring-type sub-ring
# Create ERPS instance 1.
[DeviceC-erps-ring2-inst1] instance 1
# Configure the node role.
[DeviceC-erps-ring2-inst1] node-role interconnection port0
# Configure the control VLAN.
[DeviceC-erps-ring2-inst1] control-vlan 110
# Configure the protected VLANs.
[DeviceC-erps-ring2-inst1] protected-vlan reference-instance 1
# Enable ERPS for instance 1.
[DeviceC-erps-ring2-inst1] instance enable
[DeviceC-erps-ring2-inst1] quit
# Create Ethernet service instance 5, in which the MA is identified by a VLAN and serves VLAN 5.

```plaintext
[DeviceC] cfd service-instance 5 ma-id vlan-based md MD_A vlan 5
```

# Configure a MEP list in Ethernet service instance 5, create outward-facing MEP 5001 in Ethernet service instance 3, and enable CCM sending on GigabitEthernet 1/0/3.

```plaintext
[DeviceC] cfd meplist 5001 5002 service-instance 5
[DeviceC-GigabitEthernet1/0/3] cfd mep 5001 service-instance 5 outbound
[DeviceC-GigabitEthernet1/0/3] cfd cc service-instance 5 mep 5001 enable
```

# Create track entry 1 and associate it with the CC function of CFD for MEP 5001 in Ethernet service instance 3.

```plaintext
[DeviceC] track 1 cfd cc service-instance 5 mep 5001
```

# Associate GigabitEthernet 1/0/3 with track entry 1 and bring up the port.

```plaintext
[DeviceC-GigabitEthernet1/0/3] port erps ring 2 instance 1 track 1
[DeviceC-GigabitEthernet1/0/3] undo shutdown
```

# Enable ERPS.

```plaintext
[DeviceC-GigabitEthernet1/0/3] quit
```

# Enable ERPS.

```plaintext
[DeviceC] erps enable
```

4. **Configure Device D.**

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

```plaintext
<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
```

# Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```plaintext
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] link-delay 0
```

# Disable the spanning tree feature on the port.

```plaintext
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

# Configure the port as a trunk port and assign it to VLANs 1 to 30.

```plaintext
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```plaintext
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] link-delay 0
[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
```

# Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.

```plaintext
[DeviceD] interface gigabitethernet 1/0/3
```

127
[DeviceD-GigabitEthernet1/0/3] link-delay 0
[DeviceD-GigabitEthernet1/0/3] undo stp enable
[DeviceD-GigabitEthernet1/0/3] port link-type trunk
[DeviceD-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/3] quit

# Create ERPS ring 1.
[DeviceD] erps ring 1

# Configure ERPS ring member ports.
[DeviceD-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceD-erps-ring1] port1 interface gigabitethernet 1/0/2

# Create ERPS instance 1.
[DeviceD-erps-ring1] instance 1

# Configure the control VLAN.
[DeviceD-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.
[DeviceD-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.
[DeviceD-erps-ring1-inst1] instance enable
[DeviceD-erps-ring1-inst1] quit
[DeviceD-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD_A.
[DeviceD] cfd enable
[DeviceD] cfd md MD_A level 5

# Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.
[DeviceD] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2

# Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2002 in Ethernet service instance 2, and enable CCM sending on GigabitEthernet 1/0/2.
[DeviceD] cfd meplist 2001 2002 service-instance 2
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] cfd mep 2002 service-instance 2 outbound
[DeviceD-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2002 enable
[DeviceD-GigabitEthernet1/0/2] quit

# Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.
[DeviceD] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4

# Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4002 in Ethernet service instance 4, and enable CCM sending on GigabitEthernet 1/0/1.
[DeviceD] cfd meplist 4001 4002 service-instance 4
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd mep 4002 service-instance 4 outbound
[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4002 enable
[DeviceD-GigabitEthernet1/0/1] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 2002 in Ethernet service instance 2.
[DeviceD] track 1 cfd cc service-instance 2 mep 2002

# Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port.
[DeviceD] interface gigabitethernet 1/0/2
Create track entry 2 and associate it with the CC function of CFD for MEP 4002 in Ethernet service instance 4.

DeviceD: track 2 cfd cc service-instance 4 mep 4002

Associate GigabitEthernet 1/0/1 with track entry 2 and bring up the port.

DeviceD: interface gigabitethernet 1/0/1
DeviceD-GigabitEthernet1/0/1: port erps ring 1 instance 1 track 2
DeviceD-GigabitEthernet1/0/1: undo shutdown
DeviceD-GigabitEthernet1/0/1: quit

Create ERPS ring 2.

DeviceD: erps ring 2

Configure ERPS ring member ports.

DeviceD-erps-ring2: port0 interface gigabitethernet 1/0/3

Configure ERPS ring 2 as the subring.

DeviceD-erps-ring2: ring-type sub-ring

Create ERPS instance 1.

DeviceD-erps-ring2: instance 1

Configure the node role.

DeviceD-erps-ring2-inst1: node-role interconnection port0

Configure the control VLAN.

DeviceD-erps-ring2-inst1: control-vlan 110

Configure the protected VLANs.

DeviceD-erps-ring2-inst1: protected-vlan reference-instance 1

Enable ERPS for instance 1.

DeviceD-erps-ring2-inst1: instance enable
DeviceD-erps-ring2-inst1: quit
DeviceD-erps-ring2: quit

Create Ethernet service instance 6, in which the MA is identified by a VLAN and serves VLAN 6.

DeviceD: cfd service-instance 6 ma-id vlan-based md MD_A vlan 6

Configure a MEP list in Ethernet service instance 6, create outward-facing MEP 6002 in Ethernet service instance 3, and enable CCM sending on GigabitEthernet 1/0/3.

DeviceD: cfd meplist 6001 6002 service-instance 6
DeviceD: interface gigabitethernet 1/0/3
DeviceD-GigabitEthernet1/0/3: cfd mep 6002 service-instance 6 outbound
DeviceD-GigabitEthernet1/0/3: cfd cc service-instance 6 mep 6002 enable
DeviceD-GigabitEthernet1/0/3: quit

Create track entry 1 and associate it with the CC function of CFD for MEP 6002 in Ethernet service instance 6.

DeviceD: track 1 cfd cc service-instance 6 mep 6002

Associate GigabitEthernet 1/0/3 with track entry 1 and bring up the port.

DeviceD: interface gigabitethernet 1/0/3
DeviceD-GigabitEthernet1/0/3: port erps ring 2 instance 1 track 1
DeviceD-GigabitEthernet1/0/3: undo shutdown
DeviceD-GigabitEthernet1/0/3: quit

Enable ERPS.
Configure Device E.

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

```plaintext
<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

# Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceE-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 30.
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/1] quit

# Create ERPS ring 2.
[DeviceE] erps ring 2

# Configure ERPS ring member ports.
[DeviceE-erps-ring2] port0 interface gigabitethernet 1/0/1
[DeviceE-erps-ring2] port1 interface gigabitethernet 1/0/2

# Configure ERPS ring 2 as the subring.
[DeviceE-erps-ring2] ring-type sub-ring

# Create ERPS instance 1.
[DeviceE-erps-ring2] instance 1

# Configure the node role.
[DeviceE-erps-ring2-inst1] node-role owner rpl port0

# Configure the control VLAN.
[DeviceE-erps-ring2-inst1] control-vlan 110

# Configure the protected VLANs.
[DeviceE-erps-ring2-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.
[DeviceE-erps-ring2-inst1] instance enable
[DeviceE-erps-ring2-inst1] quit
[DeviceE-erps-ring2] quit

# Enable CFD, and create a level-5 MD named MD_A.
[DeviceE] cfd enable
```
# Create Ethernet service instance 6, in which the MA is identified by a VLAN and serves VLAN 6.
[DeviceE] cfd service-instance 6 ma-id vlan-based md MD_A vlan 6
# Configure a MEP list in Ethernet service instance 6, create outward-facing MEP 6001 in Ethernet service instance 6, and enable CCM sending on GigabitEthernet 1/0/2.
[DeviceE] cfd meplist 6001 6002 service-instance 6
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] cfd mep 6001 service-instance 6 outbound
[DeviceE-GigabitEthernet1/0/2] cfd cc service-instance 6 mep 6001 enable
[DeviceE-GigabitEthernet1/0/2] quit
# Create Ethernet service instance 7, in which the MA is identified by a VLAN and serves VLAN 7.
[DeviceE] cfd service-instance 7 ma-id vlan-based md MD_A vlan 7
# Configure a MEP list in Ethernet service instance 7, create outward-facing MEP 7001 in Ethernet service instance 7, and enable CCM sending on GigabitEthernet 1/0/1.
[DeviceE] cfd meplist 7001 7002 service-instance 7
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] cfd mep 7001 service-instance 7 outbound
[DeviceE-GigabitEthernet1/0/1] cfd cc service-instance 7 mep 7001 enable
[DeviceE-GigabitEthernet1/0/1] quit
# Create track entry 1 and associate it with the CC function of CFD for MEP 6001 in Ethernet service instance 6.
[DeviceE] track 1 cfd cc service-instance 6 mep 6001
# Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port.
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] port erps ring 2 instance 1 track 1
[DeviceE-GigabitEthernet1/0/2] undo shutdown
[DeviceE-GigabitEthernet1/0/2] quit
# Create track entry 2 and associate it with the CC function of CFD for MEP 7001 in Ethernet service instance 7.
[DeviceE] track 2 cfd cc service-instance 7 mep 7001
# Associate GigabitEthernet 1/0/1 with track entry 2 and bring up the port.
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] port erps ring 2 instance 1 track 2
[DeviceE-GigabitEthernet1/0/1] undo shutdown
[DeviceE-GigabitEthernet1/0/1] quit
# Enable ERPS.
[DeviceE] erps enable

6. Configure Device F.
# Create VLANs 1 to 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
# Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceF-GigabitEthernet1/0/1] undo stp enable
[DeviceF-GigabitEthernet1/0/1] port link-type trunk

# Configure the port as a trunk port and assign it to VLANs 1 to 30.
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceF-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] link-delay 0
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[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 ERPS ring 2.
[DeviceF] erps ring 2

# Configure ERPS ring member ports.
[DeviceF-erps-ring2] port0 interface gigabitethernet 1/0/1
[DeviceF-erps-ring2] port1 interface gigabitethernet 1/0/2

# Configure ERPS ring 2 as the subring.
[DeviceF-erps-ring2] ring-type sub-ring

# Create ERPS instance 1.
[DeviceF-erps-ring2] instance 1

# Configure the node role.
[DeviceF-erps-ring2] node-role neighbor rpl port0

# Configure the control VLAN.
[DeviceF-erps-ring2-inst1] control-vlan 110

# Configure the protected VLANs.
[DeviceF-erps-ring2-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.
[DeviceF-erps-ring2-inst1] instance enable
[DeviceF-erps-ring2-inst1] quit
[DeviceF-erps-ring2] quit

# Enable CFD, and create a level-5 MD named MD_A.
[DeviceF] cfd enable
[DeviceF] cfd md MD_A level 5

# Create Ethernet service instance 5, in which the MA is identified by a VLAN and serves VLAN 5.
[DeviceF] cfd service-instance 5 ma-id vlan-based md MD_A vlan 5

# Configure a MEP list in Ethernet service instance 5, create outward-facing MEP 5002 in Ethernet service instance 5, and enable CCM sending on GigabitEthernet 1/0/2.
[DeviceF] cfd meplist 5001 5002 service-instance 5
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] cfd mep 5002 service-instance 5 outbound
[DeviceF-GigabitEthernet1/0/2] cfd cc service-instance 5 mep 5002 enable
# Create Ethernet service instance 7, in which the MA is identified by a VLAN and serves VLAN 7.
[DeviceF] cfd service-instance 7 ma-id vlan-based md MD_A vlan 7

# Configure a MEP list in Ethernet service instance 7, create outward-facing MEP 7002 in Ethernet service instance 7, and enable CCM sending on GigabitEthernet 1/0/1.
[DeviceF] cfd meplist 7001 7002 service-instance 7
[DeviceF-GigabitEthernet1/0/1] cfd mep 7002 service-instance 7 outbound
[DeviceF-GigabitEthernet1/0/1] cfd cc service-instance 7 mep 7002 enable

# Create track entry 1 and associate it with the CC function of CFD for MEP 5001 in Ethernet service instance 5.
[DeviceF] track 1 cfd cc service-instance 5 mep 5002

# Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port.
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] port erps ring 2 instance 1 track 1
[DeviceF-GigabitEthernet1/0/2] undo shutdown

# Create track entry 2 and associate it with the CC function of CFD for MEP 7002 in Ethernet service instance 7.
[DeviceF] track 2 cfd cc service-instance 7 mep 7002

# Associate GigabitEthernet 1/0/1 with track entry 2 and bring up the port.
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] port erps ring 2 instance 1 track 2
[DeviceF-GigabitEthernet1/0/1] undo shutdown

# Enable ERPS.
[DeviceF] erps enable

Verifying the configuration

# Display information about ERPS instance 1 for Device A.
[Device A] display erps detail ring 1

Verifying the configuration
Enable status : Yes, Active status : Yes
R-APS level : 7

<table>
<thead>
<tr>
<th>Port</th>
<th>PortRole</th>
<th>PortStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port0</td>
<td>RPL</td>
<td>Block</td>
</tr>
<tr>
<td>Port1</td>
<td>Non-RPL</td>
<td>Up</td>
</tr>
</tbody>
</table>

The output shows the following information:
- Device A is the owner node.
- The ERPS ring is in idle state.
- The RPL port is blocked.
- The non-RPL port is unblocked.

One-ring multi-instance load balancing configuration example

**Network requirements**

As shown in Figure 36, perform the following tasks to improve network resource utilization and implement load balancing among links:

- Configure ERPS instances 1 and 2 on the ERPS ring.
- For ERPS instance 1, configure the following items:
  - Configure Device A as the owner node.
  - Configure VLAN 100 as the control VLAN.
  - Configure VLANs 1 to 30 as the protected VLANs.
- For ERPS instance 2, configure the following items:
  - Configure Device A as the owner node.
  - Configure VLAN 100 as the control VLAN.
  - Configure VLANs 31 to 60 as the protected VLANs.

**Figure 36 Network diagram**

![Network diagram](image)

**Configuration procedure**

1. Configure Device A.
# Create VLANs 1 to 60, map VLANs 1 to 30 to MSTI 1, map VLANs 31 to 60 to MSTI 2, and activate the MST region configuration.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 60
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1 to 30
[DeviceA-mst-region] instance 2 vlan 31 to 60
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

# Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] link-delay 0
```

# Disable the spanning tree feature on the port.

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

# Configure the port as a trunk port and assign it to VLANs 1 to 60.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 60
[DeviceA-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 60
[DeviceA-GigabitEthernet1/0/2] quit
```

# Create ERPS ring 1.

```
[DeviceA] erps ring 1
```

# Configure ERPS ring member ports.

```
[DeviceA-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceA-erps-ring1] port1 interface gigabitethernet 1/0/2
```

# Create ERPS instance 1.

```
[DeviceA-erps-ring1] instance 1
```

# Configure the node role.

```
[DeviceA-erps-ring1-inst1] node-role owner rpl port0
```

# Configure the control VLAN.

```
[DeviceA-erps-ring1-inst1] control-vlan 100
```

# Configure the protected VLANs.

```
[DeviceA-erps-ring1-inst1] protected-vlan reference-instance 1
```

# Enable ERPS for instance 1.

```
[DeviceA-erps-ring1-inst1] instance enable
[DeviceA-erps-ring1-inst1] quit
[DeviceA-erps-ring1] quit
```

# Create ERPS instance 2.

```
[DeviceA-erps-ring1] instance 2
```

# Configure the control VLAN.

```
[DeviceA-erps-ring1-inst2] control-vlan 110
```

# Configure the protected VLANs.
# Enable ERPS for instance 2.
[DeviceA-erps-ring1-inst2] instance enable
[DeviceA-erps-ring1-inst2] quit
[DeviceA-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD_A.
[DeviceA] cfd enable
[DeviceA] cfd md MD_A level 5

# Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.
[DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1

# Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1001 in Ethernet service instance 1, and enable CCM sending 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 1001 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] quit

# Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.
[DeviceA] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2

# Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2001 in Ethernet service instance 1, and enable CCM sending 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 2001 service-instance 2 outbound
[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceA-GigabitEthernet1/0/2] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 1001 in Ethernet service instance 1.
[DeviceA] track 1 cfd cc service-instance 1 mep 1001

# Associate GigabitEthernet 1/0/1 with track entry 1 and bring up the port for ERPS instances 1 and 2.
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceA-GigabitEthernet1/0/1] port erps ring 1 instance 2 track 1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 2001 in Ethernet service instance 2.
[DeviceA] track 2 cfd cc service-instance 2 mep 2001

# Associate GigabitEthernet 1/0/2 with track entry 2 and bring up the port for ERPS instances 1 and 2.
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceA-GigabitEthernet1/0/2] port erps ring 1 instance 2 track 2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
[DeviceA-GigabitEthernet1/0/2] quit

# Enable ERPS.
2. Configure Device B.

# Create VLANs 1 to 60, map VLANs 1 to 30 to MSTI 1, map VLANs 31 to 60 to MSTI 2, and activate the MST region configuration.

```mpls
<DeviceB> system-view
[DeviceB] vlan 1 to 60
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
[DeviceB-mst-region] instance 2 vlan 31 to 60
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

# Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```mpls
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0
```

# Disable the spanning tree feature on the port.

```mpls
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

# Configure the port as a trunk port and assign it to VLANs 1 to 60.

```mpls
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 60
[DeviceB-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```mpls
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 60
[DeviceB-GigabitEthernet1/0/2] quit
```

# Create ERPS ring 1.

```mpls
[DeviceB] erps ring 1
```

# Configure ERPS ring member ports.

```mpls
[DeviceB-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceB-erps-ring1] port1 interface gigabitethernet 1/0/2
```

# Create ERPS instance 1.

```mpls
[DeviceB-erps-ring1-inst1] instance 1
```

# Configure the node role.

```mpls
[DeviceB-erps-ring1-inst1] node-role neighbor rpl port0
```

# Configure the control VLAN.

```mpls
[DeviceB-erps-ring1-inst1] control-vlan 100
```

# Configure the protected VLANs.

```mpls
[DeviceB-erps-ring1-inst1] protected-vlan reference-instance 1
```

# Enable ERPS for instance 1.

```mpls
[DeviceB-erps-ring1-inst1] instance enable
[DeviceB-erps-ring1-inst1] quit
```

# Create ERPS instance 2.

```mpls
[DeviceB-erps-ring1] instance 2
```

# Configure the control VLAN.
# Configure the protected VLANs.
[DeviceB-erps-ring1-inst2] control-vlan 110

# Enable ERPS for instance 2.
[DeviceB-erps-ring1-inst2] instance enable
[DeviceB-erps-ring1-inst2] quit
[DeviceB-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD_A.
[DeviceB] cfd enable
[DeviceB] cfd md MD_A level 5

# Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.
[DeviceB] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1

# Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1002 in Ethernet service instance 1, and enable CCM sending on GigabitEthernet 1/0/1.
[DeviceB] cfd meplist 1001 1002 service-instance 1
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound
[DeviceB-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable

# Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.
[DeviceB] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3

# Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3002 in Ethernet service instance 3, and enable CCM sending on GigabitEthernet 1/0/2.
[DeviceB] cfd meplist 3001 3002 service-instance 3
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] cfd mep 3002 service-instance 3 outbound
[DeviceB-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3002 enable

# Create track entry 1 and associate it with the CC function of CFD for MEP 1002 in Ethernet service instance 1.
[DeviceB] track 1 cfd cc service-instance 1 mep 1002

# Associate GigabitEthernet 1/0/1 with track entry 1 and bring up the port for ERPS instances 1 and 2.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceB-GigabitEthernet1/0/1] port erps ring 1 instance 2 track 1
[DeviceB-GigabitEthernet1/0/1] undo shutdown

# Create track entry 2 and associate it with the CC function of CFD for MEP 3002 in Ethernet service instance 3.
[DeviceB] track 2 cfd cc service-instance 3 mep 3002

# Associate GigabitEthernet 1/0/2 with track entry 2 and bring up the port for ERPS instances 1 and 2.
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceB-GigabitEthernet1/0/2] port erps ring 1 instance 2 track 2
[DeviceB-GigabitEthernet1/0/2] undo shutdown
3. Configure Device C.

# Enable ERPS.
[DeviceB] erps enable

# Create VLANs 1 to 60, map VLANs 1 to 30 to MSTI 1, map VLANs 31 to 60 to MSTI 2, and activate the MST region configuration.
<DeviceC> system-view
[DeviceC] vlan 1 to 60
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
[DeviceC-mst-region] instance 2 vlan 31 to 60
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit

# Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceC-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 60.
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 60
[DeviceC-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] link-delay 0
[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 60
[DeviceC-GigabitEthernet1/0/2] quit

# Create ERPS ring 1.
[DeviceC] erps ring 1

# Configure ERPS ring member ports.
[DeviceC-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceC-erps-ring1] port1 interface gigabitethernet 1/0/2

# Create ERPS instance 1.
[DeviceC-erps-ring1] instance 1

# Configure the control VLAN.
[DeviceC-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.
[DeviceC-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.
[DeviceC-erps-ring1-inst1] instance enable
[DeviceC-erps-ring1-inst1] quit
[DeviceC-erps-ring1] quit

# Create ERPS instance 2.
[DeviceC-erps-ring1] instance 2

# Configure the node role.
[DeviceC-erps-ring1-inst2] node-role owner rpl port0

# Configure the control VLAN.
[DeviceC-erps-ring1-inst2] control-vlan 110

# Configure the protected VLANs.
[DeviceC-erps-ring1-inst2] protected-vlan reference-instance 2

# Enable ERPS for instance 2.
[DeviceC-erps-ring1-inst2] instance enable
[DeviceC-erps-ring1-inst2] quit

[DeviceC-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD_A.
[DeviceC] cfd enable
[DeviceC] cfd md MD_A level 5

# Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.
[DeviceC] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3

# Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3001 in Ethernet service instance 3, and enable CCM sending on GigabitEthernet 1/0/2.
[DeviceC] cfd meplist 3001 3002 service-instance 3
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd mep 3001 service-instance 3 outbound
[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3001 enable
[DeviceC-GigabitEthernet1/0/2] quit

# Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.
[DeviceC] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4

# Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4001 in Ethernet service instance 4, and enable CCM sending on GigabitEthernet 1/0/1.
[DeviceC] cfd meplist 4001 4002 service-instance 4
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 4001 service-instance 4 outbound
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4001 enable
[DeviceC-GigabitEthernet1/0/1] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 3001 in Ethernet service instance 3.
[DeviceC] track 1 cfd cc service-instance 3 mep 3001

# Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port for ERPS instances 1 and 2.
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceC-GigabitEthernet1/0/2] port erps ring 1 instance 2 track 1
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 4001 in Ethernet service instance 4.
[DeviceC] track 2 cfd cc service-instance 4 mep 4001

# Associate GigabitEthernet 1/0/1 with track entry 2 and bring up the port for ERPS instances 1 and 2.
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceC-GigabitEthernet1/0/1] port erps ring 1 instance 2 track 2
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit

# Enable ERPS.
[DeviceC] erps enable

4. Configure Device D.

# Create VLANs 1 to 60, map VLANs 1 to 30 to MSTI 1, map VLANs 31 to 60 to MSTI 2, and activate the MST region configuration.
<DeviceD> system-view
[DeviceD] vlan 1 to 60
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30
[DeviceD-mst-region] instance 2 vlan 31 to 60
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit

# Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] link-delay 0

# Disable the spanning tree feature on the port.
[DeviceD-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port and assign it to VLANs 1 to 60.
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 60
[DeviceD-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] link-delay 0
[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 60
[DeviceD-GigabitEthernet1/0/2] quit

# Create ERPS ring 1.
[DeviceD] erps ring 1

# Configure ERPS ring member ports.
[DeviceD-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceD-erps-ring1] port1 interface gigabitethernet 1/0/2

# Create ERPS instance 1.
[DeviceD-erps-ring1] instance 1

# Configure the control VLAN.
[DeviceD-erps-ring1-inst1] control-vlan 100

# Configure the protected VLANs.
[DeviceD-erps-ring1-inst1] protected-vlan reference-instance 1

# Enable ERPS for instance 1.
[DeviceD-erps-ring1-inst1] instance enable
[DeviceD-erps-ring1-inst1] quit
[DeviceD-erps-ring1] quit

# Create ERPS instance 2.
# Configure the node role.
[DeviceD-erps-ring1-inst2] node-role neighbor rpl port0

# Configure the control VLAN.
[DeviceD-erps-ring1-inst2] control-vlan 110

# Configure the protected VLANs.

# Enable ERPS for instance 2.
[DeviceD-erps-ring1-inst2] instance enable
[DeviceD-erps-ring1-inst2] quit
[DeviceD-erps-ring1] quit

# Enable CFD, and create a level-5 MD named MD_A.
[DeviceD] cfd enable
[DeviceD] cfd md MD_A level 5

# Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.
[DeviceD] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2

# Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2002 in Ethernet service instance 2, and enable CCM sending on GigabitEthernet 1/0/2.
[DeviceD] cfd meplist 2001 2002 service-instance 2
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] cfd mep 2002 service-instance 2 outbound
[DeviceD-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2002 enable
[DeviceD-GigabitEthernet1/0/2] quit

# Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.
[DeviceD] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4

# Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4002 in Ethernet service instance 4, and enable CCM sending on GigabitEthernet 1/0/1.
[DeviceD] cfd meplist 4001 4002 service-instance 4
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd mep 4002 service-instance 4 outbound
[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4002 enable
[DeviceD-GigabitEthernet1/0/1] quit

# Create track entry 1 and associate it with the CC function of CFD for MEP 2002 in Ethernet service instance 2.
[DeviceD] track 1 cfd cc service-instance 2 mep 2002

# Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port for ERPS instances 1 and 2.
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceD-GigabitEthernet1/0/2] port erps ring 1 instance 2 track 1
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] quit

# Create track entry 2 and associate it with the CC function of CFD for MEP 4002 in Ethernet service instance 4.
[DeviceD] track 2 cfd cc service-instance 4 mep 4002
# Associate GigabitEthernet 1/0/1 with track entry 2 and bring up the port for ERPS instances 1 and 2.

[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceD-GigabitEthernet1/0/1] port erps ring 1 instance 2 track 2
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] quit

# Enable ERPS.
[DeviceD] erps enable

Verifying the configuration

# Display information about ERPS instance 1 for Device A.
[Device A] display erps detail ring 1

<table>
<thead>
<tr>
<th>Port ID</th>
<th>PortRole</th>
<th>PortStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port0</td>
<td>RPL</td>
<td>Block</td>
</tr>
<tr>
<td>Port1</td>
<td>Non-RPL</td>
<td>Up</td>
</tr>
</tbody>
</table>

Instance ID : 1
Node role : Owner
Node state : Idle
Connect(ring/instance): -
Control VLAN : 100
Protected VLAN : Reference-instance 1
Guard timer : 500 ms
Hold-off timer : 0 ms
WTR timer : 5 min
Revertive operation : Revertive
Enable status : Yes, Active status : Yes
R-APS level : 7

<table>
<thead>
<tr>
<th>Port</th>
<th>PortRole</th>
<th>PortStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port0</td>
<td>RPL</td>
<td>Block</td>
</tr>
<tr>
<td>Port1</td>
<td>Non-RPL</td>
<td>Up</td>
</tr>
</tbody>
</table>

Instance ID : 2
Node role : Normal
Node state : Idle
Connect(ring/instance): -
Control VLAN : 100
Protected VLAN : Reference-instance 2
Guard timer : 500 ms
Hold-off timer : 0 ms
WTR timer : 5 min
Revertive operation : Revertive
Enable status : Yes, Active status : Yes
R-APS level : 7
Port PortRole PortStatus
The output shows the following information:

- For ERPS instance 1:
  - Device A is the owner node.
  - The ERPS ring is in idle state.
  - The RPL port is blocked.
  - The non-RPL port is unblocked.

- For ERPS instance 2:
  - Device A is a normal node.
  - The ERPS ring is in idle state.
  - The non-RPL port is unblocked.

## Troubleshooting ERPS

### Symptom

The link between the owner node and the faulty node is available, but the owner node cannot receive SF packets sent by the faulty node. The RPL port is blocked.

### Analysis

Possible reasons include:

- ERPS is not enabled for some nodes on the ERPS ring.
- The ring IDs are different for the nodes on the same ERPS ring.
- The control VLAN IDs are different for the nodes in the same ERPS instance.
- The RPL port is faulty.

### Solutions

To resolve the problem:

- Use the `display erps` command to examine whether ERPS is enabled for all nodes on the ERPS ring. If ERPS is disabled for some nodes, use the `erps enable` command to enable ERPS for the nodes.
- Set the same ring ID for all nodes on a ERPS ring and configure the same control VLAN for all nodes in an ERPS instance.
- Use the `display erps detail` command to examine the port status for all nodes. Bring up the ports in down state.
- Use the `debugging erps` command on all nodes to view debugging information about packets and node status.
Configuring Smart Link

Overview

To avoid single-point failures and guarantee network reliability, downstream devices are usually dual-homed to upstream devices, as shown in Figure 37.

Figure 37 Dual uplink network diagram

To remove network loops on a dual-homed network, you can use a spanning tree protocol or the Rapid Ring Protection Protocol (RRPP). However, convergence time is long with spanning tree protocols, which makes it unsuitable for users who have high demand on convergence speed. RRPP can meet demand on convergence speed, but it involves complicated networking and configurations and is mainly used in ring-shaped networks.

For more information about spanning tree protocols, see Layer 2—LAN Switching Configuration Guide. For more information about RRPP, see "Configuring RRPP."

Smart Link is a feature developed to address the slow convergence issue with STP. It provides link redundancy and fast convergence in a dual uplink network, allowing the backup link to take over quickly when the primary link fails. Smart Link features subsecond convergence time.

A Smart Link device is configured with a smart link group and a transmit control VLAN to transmit flush messages. For example, Device C and Device D in Figure 37 are Smart Link devices.

An associated device supports Smart Link, and receives flush messages sent from the specified control VLAN. For example, Device A, Device B, and Device E in Figure 37 are associated devices.
Terminology

Smart link group
A smart link group consists of only two member ports: the primary and the secondary ports. Only one port is active for forwarding at a time, and the other port is blocked and in standby state. When link failure occurs on the active port due to port shutdown or the presence of unidirectional link, the standby port becomes active and takes over. The original active port transits to the blocked state.

As shown in Figure 37, Port 1 and Port 2 of Device C form a smart link group and those of Device D form another. Port 1 is active and Port 2 is standby.

Primary/secondary port
Primary port and secondary port are two port types in a smart link group. When both ports in a smart link group are up, the primary port preferentially transits to the forwarding state. The secondary port stays in standby state. When the primary port fails, the secondary port takes over to forward traffic.

As shown in Figure 37, Port 1 of Device C and that of Device D are primary ports. Port 2 of Device C and that of Device D are secondary ports.

Primary/secondary link
The link that connects the primary port in a smart link group is the primary link. The link that connects the secondary port is the secondary link.

Flush message
When link switchover occurs, the smart link group uses flush messages to notify other devices to refresh their MAC address entries and ARP/ND entries. 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 protected VLANs. Each smart link group on a port controls a different protected VLAN. 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 37) send 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 37) receive and process flush messages in the receive control VLAN. In addition, they refresh their MAC address entries and ARP/ND entries.

How Smart Link works

Link backup
As shown in Figure 37, the link on Port 1 of Device C is the primary link. The link on Port 2 of Device C is the secondary link. Port 1 is in forwarding state, and Port 2 is in standby state. When the primary link fails, Port 2 takes over to forward traffic and Port 1 is blocked and placed in standby state.

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

Link switchover might outdate the MAC address entries and ARP/ND entries on all devices. The following entry update mechanisms are provided to ensure correct packet transmission:

- **Uplink traffic-triggered MAC address learning**—Update is triggered by uplink traffic. This mechanism is applicable to environments with devices that do not support Smart Link, including devices from other vendors.

- **Flush update**—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 their MAC address forwarding entries and ARP/ND entries.

Preemption mode

As shown in Figure 37, the link on Port 1 of Device C is the primary link. The link on Port 2 of Device C is the secondary link. When the primary link fails, Port 1 is automatically blocked and placed in standby state, and Port 2 takes over to forward traffic. When the primary link recovers, one of the following actions occurs:

- If the smart link group is not configured with a preemption mode, Port 1 stays blocked to keep traffic forwarding stable. Port 1 does not take over to forward traffic until the next link switchover.

- If the smart link group is configured with a preemption mode and the preemption conditions are met, Port 1 takes over to forward traffic as soon as its link recovers. Port 2 is automatically blocked and placed in standby state.

Load sharing

A ring network might carry traffic of multiple VLANs. Smart Link can forward traffic from different VLANs in different smart link groups for load sharing.

To implement load sharing, you can assign a port to multiple smart link groups. Configure each group with a different protected VLAN. Make sure the state of the port is different in these smart link groups, so traffic from 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). For more information about MSTIs, see *Layer 2—LAN Switching Configuration Guide*.

Smart Link collaboration mechanisms

Collaboration between Smart Link and Monitor Link

Smart Link cannot detect when faults occur on the uplink of the upstream devices or when faults are cleared. You can configure the Monitor Link function to monitor the status of the uplink ports of the upstream devices. Monitor Link adapts the up/down state of downlink ports to uplink ports, and triggers 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 Track

Smart Link cannot detect unidirectional links, misconnected fibers, or packet loss on intermediate devices or network paths of the uplink. It cannot detect when faults are cleared either. To detect link status, smart link group member 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.

Smart Link collaborates with link detection protocols through track entries. It supports only the Continuity Check (CC) function of Connectivity Fault Detection (CFD) to implement link detection. CFD notifies the smart link group member ports of fault detection events by using 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 track entries and the CC function of CFD, see "Configuring Track" and "Configuring CFD."
Smart Link configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuring a Smart Link device:</strong></td>
</tr>
<tr>
<td>• (Required.) Configuring protected VLANs for a smart link group</td>
</tr>
<tr>
<td>• (Required.) Configuring member ports for a smart link group</td>
</tr>
<tr>
<td>• (Optional.) Configuring a preemption mode for a smart link group</td>
</tr>
<tr>
<td>• (Optional.) Enabling the sending of flush messages</td>
</tr>
<tr>
<td>• (Optional.) Configuring collaboration between Smart Link and Track</td>
</tr>
<tr>
<td><strong>Configuring an associated device</strong></td>
</tr>
<tr>
<td>• (Required.) Enabling the receiving of flush messages</td>
</tr>
</tbody>
</table>

Configuring a Smart Link device

Configuration prerequisites

Before configuring a Smart Link device, complete the following tasks:

- To prevent loops, shut down a port before configuring it as a smart link group member. You can bring up the port only after completing the smart link group configuration.
- Disable the spanning tree feature, RRPP, and ERPS on the ports you want to add to the smart link group.

**NOTE:**

- A loop might 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.
- If you configure a port as both an aggregation group member and a smart link group member, only the aggregation group configuration takes effect. The port is not shown in the output from the `display smart-link group` command. The smart link group configuration takes effect after the port leaves the aggregation group.

Configuring protected VLANs for a smart link group

Protected VLANs are configured by referencing MSTIs. The protected VLAN configuration method varies by the spanning tree mode:

In STP, RSTP, or MSTP mode, you must manually configure the mappings between VLANs and MSTIs.

In PVST mode, the device automatically maps each VLAN to an MSTI. When the spanning tree protocol is disabled globally, all VLANs are automatically mapped to MSTI 0.

To configure the protected VLANs for a smart link group:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>2.</td>
<td>stp region-configuration</td>
<td>Skip this step if the device is operating in PVST mode. For more information about the command, see Layer 2—LAN Switching Command Reference.</td>
</tr>
<tr>
<td>3.</td>
<td>Method 1: <code>instance instance-id vlan vlan-id-list</code> &lt;br&gt;Method 2: <code>vlan-mapping modulo modulo</code></td>
<td>Skip this step if the device is operating in PVST mode. All VLANs in an MST region are mapped to CIST (MSTI 0) by default. For more information about the commands, see Layer 2—LAN Switching Command Reference.</td>
</tr>
<tr>
<td>4.</td>
<td>active region-configuration</td>
<td>Skip this step if the device is operating in PVST mode. For more information about the command, see Layer 2—LAN Switching Command Reference.</td>
</tr>
<tr>
<td>5.</td>
<td>display stp region-configuration</td>
<td>Available in any view. The output of the command includes VLAN-to-instance mappings. For more information about the command, see Layer 2—LAN Switching Command Reference.</td>
</tr>
<tr>
<td>6.</td>
<td>quit</td>
<td>Skip this step if the device is operating in PVST mode.</td>
</tr>
<tr>
<td>7.</td>
<td>smart-link group <code>group-id</code></td>
<td>N/A</td>
</tr>
<tr>
<td>8.</td>
<td>protected-vlan reference-instance <code>instance-id-list</code></td>
<td>By default, a smart link group does not have protected VLANs.</td>
</tr>
</tbody>
</table>

### 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>smart-link group <code>group-id</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>`port interface-type interface-number { primary</td>
<td>secondary }`</td>
</tr>
</tbody>
</table>
In interface view

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure member ports for a smart link group.</td>
<td>port smart-link group group-id { primary</td>
</tr>
</tbody>
</table>

Configuring a preemption mode for a smart link group

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter smart link group view.</td>
<td>smart-link group group-id</td>
</tr>
<tr>
<td>3.</td>
<td>Configure a preemption mode for the smart link group.</td>
<td>preemption mode { role</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the preemption delay.</td>
<td>preemption delay delay</td>
</tr>
</tbody>
</table>

Enabling the sending of flush messages

Follow these guidelines when you enable the sending of flush messages:

- The control VLAN configured for a smart link group must be different from the control VLAN 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 must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.

To enable the sending of flush messages:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter smart link group view.</td>
<td>smart-link group group-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enable flush update.</td>
<td>flush enable [ control-vlan vlan-id ]</td>
</tr>
</tbody>
</table>
Configuring collaboration between Smart Link and Track

Smart Link collaborates with the CC function of CFD through track entries to implement link detection. Before configuring the collaboration between Smart Link and Track on a port, make sure the port has been added to the specified smart link group.

To configure collaboration between Smart Link and Track:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure collaboration between Smart Link and Track on the port.</td>
<td>port smart-link group group-id track track-entry-number</td>
</tr>
</tbody>
</table>

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 forwarding state if a topology change occurs.

Enabling the receiving of flush messages

You do not need to enable all ports on the associated devices to receive flush messages. Enable the feature only on all control VLANs of ports on the primary and secondary links between the Smart Link device and the destination device.

Follow these guidelines when you enable the receiving of flush messages:

- If no control VLAN is specified for processing flush messages, the device forwards the received flush messages without any processing.
- 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 correctly.
- Make sure the control VLANs are existing VLANs, and assign the ports capable of receiving flush messages to the control VLANs.

To enable the receiving of flush messages:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
</tbody>
</table>
Step | Command | Remarks
---|---|---
3. | **smart-link flush enable** [ control-vlan vlan-id-list ] | By default, no control VLAN receives flush messages.

Displaying and maintaining Smart Link

Perform `display` commands in any view and the `reset` command in user view:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about the received flush messages.</td>
<td><code>display smart-link flush</code></td>
</tr>
<tr>
<td>Display smart link group information.</td>
<td>`display smart-link group { group-id</td>
</tr>
<tr>
<td>Clear the statistics about flush messages.</td>
<td><code>reset smart-link statistics</code></td>
</tr>
</tbody>
</table>

Smart Link configuration examples

Single smart link group configuration example

Network requirements

As shown in Figure 38:

- Device C and Device D are Smart Link devices. Device A, Device B, and Device E are associated devices. Traffic of VLANs 1 through 30 on Device C and Device D is dually uplinked to Device A.
- Configure Smart Link on Device C and Device D for dual uplink backup.

Figure 38 Network diagram

Configuration procedure

1. Configure Device C:
   
   ```
   # Create VLANs 1 through 30.
   <DeviceC> system-view
   ```
[DeviceC] vlan 1 to 30
# Map these VLANs to MSTI 1.
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
# Activate the MST region configuration.
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
# Shut down GigabitEthernet 1/0/1.
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
# Disable the spanning tree feature on the port.
[DeviceC-GigabitEthernet1/0/1] undo stp enable
# Configure the port as a trunk port.
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
# Assign the port to VLANs 1 through 30.
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 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 primary port and GigabitEthernet 1/0/2 as the secondary port for smart link group 1.
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 secondary
# 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.
<DeviceD> system-view
[DeviceD] vlan 1 to 30
# Map these VLANs to MSTI 1.
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30

# Activate the MST region configuration.
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit

# Shut down GigabitEthernet 1/0/1.
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] shutdown

# Disable the spanning tree feature on the port.
[DeviceD-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceD-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 1 through 30.
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] 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 primary port and GigabitEthernet 1/0/2 as the secondary port for smart link group 1.
[DeviceD-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceD-smlk-group1] port gigabitethernet 1/0/2 secondary

# 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.
[DeviceB] interface gigabitethernet 1/0/1
Configure Device B:

[DeviceB-GigabitEthernet1/0/1] port link-type trunk
# Assign the port to VLANs 1 through 30.
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
# Enable flush message receiving and configure VLAN 10 and VLAN 20 as the receive control VLANs on the port.
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit
# Configure GigabitEthernet 1/0/2 as a trunk port.
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
# Assign the port to VLANs 1 through 30.
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
# Enable flush message receiving and configure VLAN 20 as the receive control VLAN on the port.
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 20
[DeviceB-GigabitEthernet1/0/2] quit
# Configure GigabitEthernet 1/0/3 as a trunk port.
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
# Assign the port to VLANs 1 through 30.
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
# Disable the spanning tree feature on the port.
[DeviceB-GigabitEthernet1/0/3] undo stp enable
# Enable flush message receiving and configure VLAN 10 as the receive control VLAN on the port.
[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.
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
# Assign the port to VLANs 1 through 30.
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
# Enable flush message receiving and configure VLAN 10 and VLAN 20 as the receive control VLANs on the port.
[DeviceE-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceE-GigabitEthernet1/0/1] quit
# Configure GigabitEthernet 1/0/2 as a trunk port.
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
# Assign the port to VLANs 1 through 30.
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30

155
# Disable the spanning tree feature on the port.
[DeviceE-GigabitEthernet1/0/2] undo stp enable

# Enable flush message receiving and configure VLAN 10 as the receive control VLAN on the port.
[DeviceE-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10

# Configure GigabitEthernet 1/0/3 as a trunk port.
[DeviceE] interface gigabitethernet 1/0/3
[DeviceE-GigabitEthernet1/0/3] port link-type trunk

# Assign the port to VLANs 1 through 30.
[DeviceE-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30

# Disable the spanning tree feature on the port.
[DeviceE-GigabitEthernet1/0/3] undo stp enable

# Enable flush message receiving and configure VLAN 20 as the receive control VLAN on the port.
[DeviceE-GigabitEthernet1/0/3] smart-link flush enable control-vlan 20

5. Configure Device A:

# Create VLANs 1 through 30.
<DeviceA> system-view
[DeviceA] vlan 1 to 30

# Configure GigabitEthernet 1/0/1 as a trunk port.
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 1 through 30.
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30

# Enable flush message receiving and configure VLAN 10 and VLAN 20 as the receive control VLANs on the port.
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20

Verifying the configuration

# 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
Multiple smart link groups load sharing configuration example

Network requirements

As shown in Figure 39:
- Device C is a Smart Link device. 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.
- 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.

Configuration procedure

1. Configure Device C:
   # Create VLAN 1 through VLAN 200.
   <DeviceC> system-view
   [DeviceC] vlan 1 to 200
   # Map VLANs 1 through 100 to MSTI 1, and VLANs 101 through 200 to MSTI 2.
   [DeviceC] stp region-configuration
   [DeviceC-mst-region] instance 1 vlan 1 to 100
   [DeviceC-mst-region] instance 2 vlan 101 to 200
   # Activate the MST region configuration.
   [DeviceC-mst-region] active region-configuration
   [DeviceC-mst-region] quit
   # Shut down GigabitEthernet 1/0/1.
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
# Disable the spanning tree feature on the port.
[DeviceC-GigabitEthernet1/0/1] undo stp enable
# Configure the port as a trunk port.
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
# Assign the port to VLAN 1 through VLAN 200.
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/1] quit
# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 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 primary port and GigabitEthernet 1/0/2 as the secondary port for smart link group 1.
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 secondary
# 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 secondary port and GigabitEthernet 1/0/2 as the primary port for smart link group 2.
[DeviceC-smlk-group2] port gigabitethernet 1/0/2 primary
[DeviceC-smlk-group2] port gigabitethernet 1/0/1 secondary
# 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.
[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
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.
   [DeviceB-GigabitEthernet1/0/1] port link-type trunk
   # Assign the port to VLANs 1 through 200.
   [DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
   # Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on the port.
   [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.
   [DeviceB] interface gigabitethernet 1/0/2
   [DeviceB-GigabitEthernet1/0/2] port link-type trunk
   # Assign the port to VLANs 1 through 200.
   [DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
   # Disable the spanning tree feature on the port.
   [DeviceB-GigabitEthernet1/0/2] undo stp enable
   # Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on the port.
   [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.
   [DeviceD-GigabitEthernet1/0/1] port link-type trunk
   # Assign the port to VLANs 1 through 200.
   [DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
   # Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on the port.
   [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.
   [DeviceD] interface gigabitethernet 1/0/2
   [DeviceD-GigabitEthernet1/0/2] port link-type trunk
   # Assign the port to VLANs 1 through 200.
   [DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
   # Disable the spanning tree feature on the port.
   [DeviceD-GigabitEthernet1/0/2] undo stp enable
   # Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on the port.
4. **Configure Device A:**

   # Configure GigabitEthernet 1/0/2:
   [DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
   [DeviceD-GigabitEthernet1/0/2] quit

   # Configure GigabitEthernet 1/0/1 as a trunk port:
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] port link-type trunk

   # Assign the port to VLANs 1 through 200:
   [DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200

   # Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on the port.
   [DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
   [DeviceA-GigabitEthernet1/0/1] quit

   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] port link-type trunk
   [DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
   [DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
   [DeviceA-GigabitEthernet1/0/2] quit

**Verifying the configuration**

   # 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

<table>
<thead>
<tr>
<th>Member</th>
<th>Role</th>
<th>State</th>
<th>Flush-count</th>
<th>Last-flush-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE1/0/1</td>
<td>PRIMARY</td>
<td>ACTIVE</td>
<td>5</td>
<td>16:45:20 2012/04/21</td>
</tr>
<tr>
<td>GE1/0/2</td>
<td>SECONDARY</td>
<td>STANDBY</td>
<td>1</td>
<td>16:37:20 2012/04/21</td>
</tr>
</tbody>
</table>

   **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

<table>
<thead>
<tr>
<th>Member</th>
<th>Role</th>
<th>State</th>
<th>Flush-count</th>
<th>Last-flush-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE1/0/2</td>
<td>PRIMARY</td>
<td>ACTIVE</td>
<td>5</td>
<td>16:45:20 2012/04/21</td>
</tr>
<tr>
<td>GE1/0/1</td>
<td>SECONDARY</td>
<td>STANDBY</td>
<td>1</td>
<td>16:37:20 2012/04/21</td>
</tr>
</tbody>
</table>
# 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 2012/04/21
Device ID of the last flush packet : 000f-e23d-5af0
Control VLAN of the last flush packet : 10

Smart Link and Track collaboration configuration example

Network requirements

As shown in Figure 40:

- Device A, Device B, Device C, and Device D form maintenance domain (MD) MD_A 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 collaboration between Smart Link and the CC function of CFD through track entries to meet the following requirements:
  - Traffic of VLANs 1 through 100 is uplinked to Device A by Device C through GigabitEthernet 1/0/1 (primary 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 (primary port of smart link group 2).
  - When the link between Device C and Device A fails, traffic is quickly switched to the secondary port of each smart link group. After the fault is cleared, traffic is switched back to the primary ports.

For more information about CFD, see "Configuring CFD."

Figure 40 Network diagram

![Network diagram](image)

Configuration procedure

1. Configure Device A:

   # Create VLAN 1 through VLAN 200.

   <DeviceA> system-view
# Configure GigabitEthernet 1/0/1 as a trunk port.
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
# Assign the port to VLANs 1 through 200.
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
# Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on the port.
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceA-GigabitEthernet1/0/1] quit
# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceA-GigabitEthernet1/0/2] quit
# Enable CFD and create MD MD_A of level 5.
[DeviceA] cfd enable
[DeviceA] cfd md MD_A level 5
# Create service instance 1 in which the MA name is based on the VLAN ID in MD_A and configure the MA to serve VLAN 10.
[DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 10
# Create a MEP list in service instance 1, create 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 cc service-instance 1 mep 1002 enable
[DeviceA-GigabitEthernet1/0/1] quit
# Create service instance 2 in which the MA name is based on the VLAN ID in MD_A and configure the MA to serve VLAN 110.
[DeviceA] cfd service-instance 2 ma-id vlan-based md MD_A vlan 110
# Create a MEP list in service instance 2, create 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 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.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
# Assign the port to VLANs 1 through 200.
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
# Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on the port.
[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.
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk

# Assign the port to VLANs 1 through 200.
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200

# Disable the spanning tree feature on the port.
[DeviceB-GigabitEthernet1/0/2] undo stp enable

# Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on the port.
[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.
<DeviceC> system-view
[DeviceC] vlan 1 to 200

# Map VLANs 1 through 100 to MSTI 1 and VLANs 101 through 200 to MSTI 2.
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 100
[DeviceC-mst-region] instance 2 vlan 101 to 200

# Activate the MST region configuration.
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit

# Shut down GigabitEthernet 1/0/1.
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown

# Disable the spanning tree feature on the port.
[DeviceC-GigabitEthernet1/0/1] undo stp enable

# Configure the port as a trunk port.
[DeviceC-GigabitEthernet1/0/1] port link-type trunk

# Assign the port to VLANs 1 through 200.
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 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 primary port and GigabitEthernet 1/0/2 as the secondary port for smart link group 1.

[DeviceC-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 secondary

# 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 secondary port and GigabitEthernet 1/0/2 as the primary port for smart link group 2.

[DeviceC-smlk-group2] port gigabitethernet 1/0/2 primary
[DeviceC-smlk-group2] port gigabitethernet 1/0/1 secondary

# 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 MD MD_A of level 5.

[DeviceC] cfd enable
[DeviceC] cfd md MD_A level 5

# Create service instance 1 in which the MA name is based on the VLAN ID in MD_A and configure the MA to serve VLAN 10.

[DeviceC] cfd service-instance 1 ma-id vlan-based md MD_A vlan 10

# Create a MEP list in service instance 1. Create 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 cc service-instance 1 mep 1001 enable
[DeviceC-GigabitEthernet1/0/1] quit

# Create service instance 2 in which the MA name is based on the VLAN ID in MD_A and configure the MA to serve VLAN 110.

[DeviceC] cfd service-instance 2 ma-id vlan-based md MD_A vlan 110

# Create a MEP list in service instance 2. Create outward-facing MEP 2001. 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 cc service-instance 2 mep 2001 enable
[DeviceC-GigabitEthernet1/0/2] quit

# Create track entry 1 that is associated with the CFD CC function of MEP 1001 in service instance 1.

[DeviceC] track 1 cfd cc service-instance 1 mep 1001
Configure collaboration between the primary port GigabitEthernet 1/0/1 of smart link group 1 and the CC function of CFD through track entry 1, and bring up the port.

```DeviceC# interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port smart-link group 1 track 1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit```

Create track entry 1 that is associated with the CFD CC function of MEP 1001 in service instance 1.

```
[DeviceC] track 2 cfd cc service-instance 2 mep 2001
```

Configure collaboration between the primary port GigabitEthernet 1/0/2 of smart link group 2 and the CC function of CFD through track entry 2, and bring up the port.

```DeviceC# interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port smart-link group 2 track 2
[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.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 1 through 200.

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
```

Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on the port.

```
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
```

Configure GigabitEthernet 1/0/2 as a trunk port.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
```

Assign the port to VLANs 1 through 200.

```
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
```

Disable the spanning tree feature on the port.

```
[DeviceD-GigabitEthernet1/0/2] undo stp enable
```

Enable flush message receiving and configure VLAN 10 and VLAN 110 as the receive control VLANs on the port.

```
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
```

Verifying the configuration

When the optical fiber between Device A and Device B fails, 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

<table>
<thead>
<tr>
<th>Member</th>
<th>Role</th>
<th>State</th>
<th>Flush-count</th>
<th>Last-flush-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE1/0/1</td>
<td>PRIMARY</td>
<td>DOWN</td>
<td>5</td>
<td>16:45:20 2012/04/21</td>
</tr>
<tr>
<td>GE1/0/2</td>
<td>SECONDARY</td>
<td>ACTIVE</td>
<td>1</td>
<td>16:37:20 2012/04/21</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Member</th>
<th>Role</th>
<th>State</th>
<th>Flush-count</th>
<th>Last-flush-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE1/0/2</td>
<td>PRIMARY</td>
<td>ACTIVE</td>
<td>5</td>
<td>16:45:20 2012/04/21</td>
</tr>
<tr>
<td>GE1/0/1</td>
<td>SECONDARY</td>
<td>STANDBY</td>
<td>1</td>
<td>16:37:20 2012/04/21</td>
</tr>
</tbody>
</table>

The output shows that primary port GigabitEthernet 1/0/1 of smart link group 1 fails, and secondary port GigabitEthernet 1/0/2 is in forwarding state.
Configuring Monitor Link

Overview

Monitor Link associates the state of downlink interfaces with the state of uplink interfaces in a monitor link group. When Monitor Link shuts down the downlink interfaces because of an uplink failure, the downstream device changes connectivity to another link.

Figure 41 Monitor Link application scenario

A monitor link group contains uplink and downlink interfaces. An interface can belong to only one monitor link group.

- Uplink interfaces are the monitored interfaces. The state of a monitor link group is associated with the state of its member uplink interfaces. When the number of uplink interfaces in up state in a monitor link group is less than the specified threshold, the monitor link group goes down and shuts down its downlink interfaces. When the number of uplink interfaces in up state reaches the threshold, the monitor link group comes up and brings up all its downlink interfaces.

- Downlink interfaces are the monitoring interfaces. The state of the downlink interfaces is associated with the state of the monitor link group. When the state of the monitor link group changes, the state of its member downlink interfaces changes to be consistent with the group state.

As shown in Figure 41:

- Port 1 and Port 2 of Device B form a monitor link group.
- Port 1 and Port 2 of Device D form another monitor link group.
- Port 1 is an uplink interface on both devices, and Port 2 is a downlink interface on both devices.

A monitor link group works independently of other monitor link groups. When the number of uplink interfaces in up state in a monitor link group is less than the specified threshold, the monitor link group goes down. It forces all downlink interfaces down at the same time. When the number of uplink
interfaces in up state reaches the threshold, the monitor link group comes up and brings up all the
downlink interfaces.

Configuration restrictions and guidelines

Follow these restrictions and guidelines when you configure Monitor Link:

- Do not manually shut down or bring up the downlink interfaces in a monitor link group.
- To avoid frequent state changes of downlink interfaces in the event that uplink interfaces in the
  monitor link group flap, you can configure a switchover delay. The switchover delay is the time
  that the downlink interfaces wait before they come up following an uplink interface.

Monitor Link configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Enabling Monitor Link globally</td>
<td></td>
</tr>
<tr>
<td>(Required.) Creating a monitor link group</td>
<td></td>
</tr>
<tr>
<td>(Required.) Configuring monitor link group member interfaces</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Configuring the uplink interface threshold for triggering monitor link group state switchover</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Configuring the switchover delay for the downlink interfaces in a monitor link group</td>
<td></td>
</tr>
</tbody>
</table>

Enabling Monitor Link globally

All monitor link groups can operate only after you enable Monitor Link globally. When you disable
Monitor Link globally, all monitor link groups cannot operate and the downlink interfaces brought
down by the monitor link groups resume their original states.

To enable Monitor Link globally:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable Monitor Link globally.</td>
<td>undo monitor-link disable</td>
<td>By default, Monitor Link is enabled globally.</td>
</tr>
</tbody>
</table>

Creating a monitor link group

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Create a monitor link group and enter monitor link group view.</td>
<td>monitor-link group group-id</td>
<td>By default, no monitor link groups exist.</td>
</tr>
</tbody>
</table>
Configuring monitor link group member interfaces

You can configure member interfaces for a monitor link group in monitor link group view or interface view. Configurations made in these views have the same effect. The configuration is supported by the following interfaces:

- Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces.
- Layer 3 Ethernet interfaces/subinterfaces and Layer 3 aggregate interfaces/subinterfaces.

Follow these guidelines when you configure monitor link group member interfaces:

- If you have configured an interface as the downlink interface of a monitor link group, do not configure its subinterfaces as the uplink interfaces of any monitor link group. Otherwise, the Monitor Link operation might be interrupted.
- The state of subinterfaces is associated with the state of the interface. Do not add the interface and its subinterfaces to the same monitor link group. Otherwise, the monitor link group performance might be affected.
- Do not add an aggregate interface and its member ports to the same monitor link group. Otherwise, the Monitor Link operation might be interrupted.
- An interface can be assigned to only one monitor link group.
- To avoid undesired down/up state changes on the downlink interfaces, configure uplink interfaces before you configure downlink interfaces.

In monitor link group view

To configure member interfaces for a monitor link group in monitor link group view:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter monitor link group view.</td>
<td>monitor-link group group-id</td>
</tr>
<tr>
<td>3.</td>
<td>Configure member interfaces for the monitor link group.</td>
<td>port interface-type {interface-number</td>
</tr>
</tbody>
</table>

In interface view

To configure member interfaces for a monitor link group in interface view:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view or subinterface view.</td>
<td>interface interface-type {interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the interface as a member of a monitor link group.</td>
<td>port monitor-link group group-id {downlink</td>
</tr>
</tbody>
</table>
Configuring the uplink interface threshold for triggering monitor link group state switchover

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter monitor link group view.</td>
<td>monitor-link group group-id</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the uplink interface threshold for triggering monitor link group state switchover.</td>
<td>uplink up-port-threshold number-of-port</td>
</tr>
</tbody>
</table>

Configuring the switchover delay for the downlink interfaces in a monitor link group

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter monitor link group view.</td>
<td>monitor-link group group-id</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the switchover delay for the downlink interfaces in the monitor link group.</td>
<td>downlink up-delay delay</td>
</tr>
</tbody>
</table>

Displaying and maintaining Monitor Link

Execute the `display` command in any view:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display monitor link group information.</td>
<td>`display monitor-link group { group-id</td>
</tr>
</tbody>
</table>

Monitor Link configuration example

**Network requirements**

As shown in Figure 42:

- 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. When the link between Device A and Device B (or Device D) fails, Device C can detect the link fault. It then performs uplink switchover in the smart link group.

For more information about Smart Link, see "Configuring Smart Link."
Figure 42 Network diagram

Configuration procedure

1. Configure Device C:
   
   # Create VLANs 1 through 30.
   <DeviceC> system-view
   [DeviceC] vlan 1 to 30
   
   # Map these VLANs to MSTI 1.
   [DeviceC] stp region-configuration
   [DeviceC-mst-region] instance 1 vlan 1 to 30
   
   # Activate MST region configuration.
   [DeviceC-mst-region] active region-configuration
   [DeviceC-mst-region] quit
   
   # Shut down GigabitEthernet 1/0/1.
   [DeviceC] interface gigabitethernet 1/0/1
   [DeviceC-GigabitEthernet1/0/1] shutdown
   
   # Disable the spanning tree feature on the interface.
   [DeviceC-GigabitEthernet1/0/1] undo stp enable
   
   # Configure the interface as a trunk port.
   [DeviceC-GigabitEthernet1/0/1] port link-type trunk
   
   # Assign the interface to VLANs 1 through 30.
   [DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
   [DeviceC-GigabitEthernet1/0/1] quit
   
   # Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
   [DeviceC] interface gigabitethernet 1/0/2
   [DeviceC-GigabitEthernet1/0/2] shutdown
   [DeviceC-GigabitEthernet1/0/2] undo stp enable
   [DeviceC-GigabitEthernet1/0/2] port link-type trunk
   [DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 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-smllk-group1] protected-vlan reference-instance 1
2. Configure Device A:

# Create VLANs 1 through 30.
<DeviceA> system-view
[DeviceA] vlan 1 to 30

# Configure GigabitEthernet 1/0/1 as a trunk port.
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk

# Assign the interface to VLANs 1 through 30.
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30

# Enable flush message receiving on the interface.
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable
[DeviceA-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 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.
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk

# Assign the interface to VLANs 1 through 30.
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30

# Enable flush message receiving on the interface.
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable
[DeviceB-GigabitEthernet1/0/1] quit

# Disable the spanning tree feature on GigabitEthernet 1/0/2.
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
# Configure the interface as a trunk port.
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
# Assign the interface to VLANs 1 through 30.
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
# Enable flush message receiving on the interface.
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable
[DeviceB-GigabitEthernet1/0/2] quit
# Create monitor link group 1.
[DeviceB] monitor-link group 1
# Configure GigabitEthernet 1/0/1 as an uplink interface for monitor link group 1.
[DeviceB-mtlk-group1] port gigabitethernet 1/0/1 uplink
# Configure GigabitEthernet 1/0/2 as a downlink interface for monitor link group 1.
[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.
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
# Assign the interface to VLANs 1 through 30.
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
# Enable flush message receiving on the interface.
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable
[DeviceD-GigabitEthernet1/0/1] quit
# Disable the spanning tree feature on GigabitEthernet 1/0/2.
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo stp enable
# Configure the interface as a trunk port.
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
# Assign the interface to VLANs 1 through 30.
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
# Enable flush message receiving on the interface.
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable
[DeviceD-GigabitEthernet1/0/2] quit
# Create monitor link group 1.
[DeviceD] monitor-link group 1
# Configure GigabitEthernet 1/0/1 as an uplink interface for monitor link group 1.
[DeviceD-mtlk-group1] port gigabitethernet 1/0/1 uplink
# Configure GigabitEthernet 1/0/2 as a downlink interface for monitor link group 1.
[DeviceD-mtlk-group1] port gigabitethernet 1/0/2 downlink
[DeviceD-mtlk-group1] quit

Verifying the configuration
# When GigabitEthernet 1/0/2 on Device A goes down because of a link fault, verify information about monitor link group 1 on Device B.
### Monitor link group 1 information:

- **Group status**: UP
- **Downlink up-delay**: 0(s)
- **Last-up-time**: 16:38:26 2012/4/21
- **Last-down-time**: 16:37:20 2012/4/21
- **Up-port-threshold**: 1

<table>
<thead>
<tr>
<th>Member</th>
<th>Role</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE1/0/1</td>
<td>UPLINK</td>
<td>UP</td>
</tr>
<tr>
<td>GE1/0/2</td>
<td>DOWNLINK</td>
<td>UP</td>
</tr>
</tbody>
</table>

# Verify information about monitor link group 1 on Device D.

### Monitor link group 1 information:

- **Group status**: DOWN
- **Downlink up-delay**: 0(s)
- **Last-up-time**: 16:37:20 2012/4/21
- **Last-down-time**: 16:38:26 2012/4/21
- **Up-port-threshold**: 1

<table>
<thead>
<tr>
<th>Member</th>
<th>Role</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE1/0/1</td>
<td>UPLINK</td>
<td>DOWN</td>
</tr>
<tr>
<td>GE1/0/2</td>
<td>DOWNLINK</td>
<td>DOWN</td>
</tr>
</tbody>
</table>
Configuring VRRP

Overview

Typically, you can configure a default gateway for every host on a LAN. All packets destined for other networks are sent through the default gateway. As shown in Figure 43, when the default gateway fails, no hosts can communicate with external networks.

![Figure 43 LAN networking](image)

Using a default gateway facilitates your configuration but requires high availability. Using more egress gateways improves link availability but introduces the problem of routing among the egresses.

Virtual Router Redundancy Protocol (VRRP) is designed to address this issue. VRRP adds a group of network gateways to a VRRP group called a virtual router. The VRRP group has one master and multiple backups, and provides a virtual IP address. The hosts on the subnet use the virtual IP address as their default network gateway to communicate with external networks.

The virtual IP address of the virtual router can be either of the following IP addresses:

- Unused IP address on the subnet where the VRRP group resides.
- IP address of an interface on a router in the VRRP group.

In the latter case, the router is called the IP address owner. A VRRP group can have only one IP address owner.

VRRP avoids single points of failure and simplifies the configuration on hosts. When the master in the VRRP group on a multicast or broadcast LAN (for example, an Ethernet network) fails, another router in the VRRP group takes over. The switchover is complete without causing dynamic route recalculation, route re-discovery, gateway reconfiguration on the hosts, or traffic interruption.

VRRP operates in either of the following modes:

- **Standard mode**— Implemented based on RFCs. For more information, see "VRRP standard mode."
- **Load balancing mode**— Extends the VRRP standard mode to distribute load across VRRP group members. For more information, see "VRRP load balancing mode."

VRRP has two versions: VRRPv2 and VRRPv3. VRRPv2 supports IPv4 VRRP. VRRPv3 supports IPv4 VRRP and IPv6 VRRP.
**VRRP standard mode**

In VRRP standard mode, only the master in the VRRP group can provide gateway service. When the master fails, the backup routers elect a new master to take over for nonstop gateway service.

**Figure 44 VRRP networking**

![VRRP networking diagram](image)

As shown in Figure 44, Router A, Router B, and Router C form a virtual router, which has its own IP address. Hosts on the subnet use the virtual router as the default gateway.

The router with the highest priority among the three routers is elected as the master, and the other two are backups.

**Router priority in a VRRP group**

VRRP determines the role (master or backup) of each router in a VRRP group by priority. A router with higher priority is more likely to become the master.

A VRRP priority can be in the range of 0 to 255, and a greater number represents a higher priority. Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses, and priority 255 is for the IP address owner. The IP address owner in a VRRP group always has a running priority of 255 and acts as the master as long as it operates correctly.

**Preemption**

A router in a VRRP group operates in either non-preemptive mode or preemptive mode.

- **Non-preemptive mode**—The master router acts as the master as long as it operates correctly, even if a backup router is later assigned a higher priority. Non-preemptive mode helps avoid frequent switchover between the master and backup routers.

- **Preemptive mode**—A backup starts a new master election and takes over as master when it detects that it has a higher priority than the current master. Preemptive mode ensures that the router with the highest priority in a VRRP group always acts as the master.

**Authentication method**

To avoid attacks from unauthorized users, VRRP member routers add authentication keys in VRRP packets to authenticate one another. VRRP provides the following authentication methods:

- **Simple authentication**
The sender fills an authentication key into the VRRP packet, and the receiver compares the received authentication key with its local authentication key. If the two authentication keys match, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate and gets discarded.

- **MD5 authentication**
  The sender computes a digest for the VRRP packet by using the authentication key and MD5 algorithm, and saves the result to the packet. The receiver performs the same operation with the authentication key and MD5 algorithm, and compares the result with the content in the authentication header. If the results match, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate and gets discarded.

On a secure network, you can choose to not authenticate VRRP packets.

NOTE:
IPv4 VRRPv3 and IPv6 VRRPv3 do not support VRRP packet authentication.

### VRRP timers

**Skew_Time**

Skew_Time helps avoid the situation that multiple backups in a VRRP group become the master when the master in the VRRP group fails.

Skew_Time is not configurable; its value depends on the VRRP version.
- In VRRPv2 (described in RFC 3768), Skew_Time is \((256 – \text{Router priority})/256\).
- In VRRPv3 (described in RFC 5798), Skew_Time is \(((256 – \text{Router priority}) \times \text{VRRP advertisement interval})/256\).

**VRRP advertisement interval**

The master in a VRRP group periodically sends VRRP advertisements to declare its presence.

You can configure the interval at which the master sends VRRP advertisements. If a backup does not receive any VRRP advertisement when the timer \((3 \times \text{VRRP advertisement interval} + \text{Skew_Time})\) expires, it takes over as the master.

**VRRP preemption delay timer**

You can configure the VRRP preemption delay timer for the following purposes:
- Avoid frequent state changes among members in a VRRP group.
- Provide the backups with enough time to collect information (such as routing information).

In preempt mode, a backup does not immediately become the master after it receives an advertisement with lower priority than the local priority. Instead, it waits for a period of time (preemption delay time + Skew_Time) before taking over as the master.

### Master election

Routers in a VRRP group determine their roles by priority. When a router joins a VRRP group, it has a backup role. The router role changes according to the following situations:
- If the backup does not receive any VRRP advertisement when the timer \((3 \times \text{advertisement interval} + \text{Skew_Time})\) expires, it becomes the master.
- If the backup receives a VRRP advertisement with the same or greater priority within the timer \((3 \times \text{advertisement interval} + \text{Skew_Time})\), it remains a backup.
- If the backup receives a VRRP advertisement with a smaller priority within the timer \((3 \times \text{advertisement interval} + \text{Skew_Time})\), the following results apply:
• It remains a backup when operating in non-preemptive mode.
• It becomes the master when operating in preemptive mode.

The elected master starts a VRRP advertisement interval to periodically send VRRP advertisements to notify the backups that it is operating correctly. Each of the backups starts a timer to wait for advertisements from the master.

After a backup receives a VRRP advertisement, it compares only the priority in the packet with its own priority.

When multiple routers in a VRRP group declare that they are the master because of network problems, the one with the highest priority becomes the master. If two routers have the same priority, the one with the highest IP address becomes the master.

**VRRP tracking**

To enable VRRP tracking, configure the routers in the VRRP group to operate in preemptive mode first. This configuration ensures that only the router with the highest priority operates as the master.

The VRRP tracking function uses network quality analyzer (NQA) or bidirectional forwarding detection (BFD) to monitor the state of the master or the upstream link. The collaboration between VRRP and NQA or BFD through a track entry implements the following functions:

- Monitors the upstream link and changes the priority of the router according to the state of the link. If the upstream link fails, the hosts on the subnet cannot access external networks through the router and the state of the track entry becomes Negative. The priority of the master decreases by a specified value, and a router with a higher priority in the VRRP group becomes the master. The switchover ensures uninterrupted communication between the hosts on the subnet and external networks.
- Monitors the state of the master on the backups. When the master fails, a backup immediately takes over to ensure uninterrupted communication.

When the track entry changes from Negative to Positive or Notready, the router automatically restores its priority. For more information about track entries, see "Configuring Track."

**VRRP application**

**Master/backup**

In master/backup mode, only the master forwards packets, as shown in Figure 45. When the master fails, a new master is elected from among the backups. This mode requires only one VRRP group, and each router in the group has a different priority. The one with the highest priority becomes the master.
Assume that Router A is acting as the master to forward packets to external networks, and Router B and Router C are backups in listening state. When Router A fails, Router B and Router C elect a new master to forward packets for hosts on the subnet.

Load sharing

A router can join multiple VRRP groups. With different priorities in different VRRP groups, the router can act as the master in one VRRP group and a backup in another.

In load sharing mode, multiple VRRP groups provide gateway services. This mode requires a minimum of two VRRP groups, and each group has one master and multiple backups. The master roles in the VRRP groups are assumed by different routers, as shown in Figure 46.

A router can be in multiple VRRP groups and have a different priority in each group.

As shown in Figure 46, the following VRRP groups exist:

- **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.

To implement load sharing among Router A, Router B, and Router C, perform the following tasks:

• Configure the virtual IP addresses of VRRP group 1, 2, and 3 as default gateway IP addresses for hosts on the subnet.

• Assign the highest priority to Router A, B, and C in VRRP group 1, 2, and 3, respectively.

**VRRP load balancing mode**

In a standard-mode VRRP group, only the master can forward packets and backups are in listening state. You can create multiple VRRP groups to share traffic, but you must configure different gateways for hosts on the subnet.

In load balancing mode, a VRRP group maps its virtual IP address to multiple virtual MAC addresses, assigning one virtual MAC address to each member router. Every router in this VRRP group can forward traffic and respond to IPv4 ARP requests or IPv6 ND requests from hosts. Because their virtual MAC addresses are different, traffic from hosts is distributed across the VRRP group members. Load balancing mode simplifies configuration and improves forwarding efficiency.

VRRP load balancing mode uses the same master election, preemption, and tracking mechanisms as the standard mode. New mechanisms have been introduced to VRRP load balancing mode, as described in the following sections.

**Virtual MAC address assignment**

In load balancing mode, the master assigns virtual MAC addresses to routers in the VRRP group. The master uses different MAC addresses to respond to ARP requests or ND requests from different hosts. The backup routers, however, do not answer ARP requests or ND requests from hosts.

In an IPv4 network, a load balanced VRRP group works as follows:

1. The master assigns virtual MAC addresses to all member routers, including itself. This example assumes that the virtual IP address of the VRRP group is 10.1.1.1/24, Router A is the master, and Router B is the backup. Router A assigns 000f-e2ff-0011 for itself and 000f-e2ff-0012 for Router B. See [Figure 47](#).

[Figure 47 Virtual MAC address assignment]
2. When an ARP request arrives, the master (Router A) selects a virtual MAC address based on the load balancing algorithm to answer the ARP request. In this example, Router A returns the virtual MAC address of itself in response to the ARP request from Host A. Router A returns the virtual MAC address of Router B in response to the ARP request from Host B. See Figure 48.

![Figure 48 Answering ARP requests](image)

3. Each host sends packets to the returned MAC address. As shown in Figure 49, Host A sends packets to Router A and Host B sends packets to Router B.

![Figure 49 Sending packets to different routers for forwarding](image)

In the ARP reply sent by the master, the source MAC address in the Ethernet header is different from the sender MAC address in the message body. For the Layer 2 device to forward the ARP packet, follow these configuration guidelines on the Layer 2 device:

- Do not enable ARP packet source MAC address consistency check.
- Do not specify the `src-mac` keyword when you enable ARP packet validity check for ARP detection.
Virtual forwarder

Virtual forwarder creation

Virtual MAC addresses enable traffic distribution across routers in a VRRP group. To enable routers in the VRRP group to forward packets, VFs must be created on them. Each VF is associated with a virtual MAC address in the VRRP group and forwards packets that are sent to this virtual MAC address.

VFs are created on routers in a VRRP group, as follows:
1. The master assigns virtual MAC addresses to all routers in the VRRP group. Each member router creates a VF for this MAC address and becomes the owner of this VF.
2. Each VF owner advertises its VF information to the other member routers.
3. After receiving the VF advertisement, each of the other routers creates the advertised VF.

Eventually, every member router maintains one VF for each virtual MAC address in the VRRP group.

VF weight and priority

The weight of a VF indicates the forwarding capability of a VF. A higher weight means higher forwarding capability. When the weight is lower than the lower limit of failure, the VF cannot forward packets.

The priority of a VF determines the VF state. Among the VFs created on different member routers for the same virtual MAC address, the VF with the highest priority is in active state. This VF, known as the active virtual forwarder (AVF), forwards packets. All other VFs listen to the state of the AVF and are known as the listening virtual forwarders (LVFs). VF priority is in the range of 0 to 255, where 255 is reserved for the VF owner. When the weight of a VF owner is higher than or equal to the lower limit of failure, the priority of the VF owner is 255.

The priority of a VF is calculated based on its weight.

- If the VF weight is higher than or equal to the lower limit of failure, the following VF priorities apply:
  - On a VF owner, the VF priority is 255.
  - On a non-VF owner, the VF priority is calculated as weight/(number of local AVFs + 1).
- If the VF weight is lower than the lower limit of failure, the VF priority is 0.

VF backup

The VFs corresponding to a virtual MAC address on different routers in the VRRP group back up one another.
Figure 50 VF information

Figure 50 shows the VF table on each router in the VRRP group and how the VFs 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. Each router creates VF 1, VF 2, and VF 3 for virtual MAC addresses 000f-e2ff-0011, 000f-e2ff-0012, and 000f-e2ff-0013, respectively. The VFs for the same virtual MAC address on different routers back up one another. For example, the VF 1 instances on Router A, Router B, and Router C back up one another.

- The VF 1 instance on Router A (the VF 1 owner) has priority 255. It acts as the AVF to forward packets sent to virtual MAC address 000f-e2ff-0011.
- The VF 1 instances on Router B and Router C have a priority of 255/(1 + 1), or 127. Because their priorities are lower than the priority of the VF 1 instance on Router A, they act as LVFs. These LVFs listen to the state of the VF 1 instance on Router A.
- When the VF 1 instance on Router A fails, the VF 1 instances on Router B and Router C elect the one with higher priority as the new AVF. This AVF forwards packets destined for virtual MAC address 000f-e2ff-0011. If the two LVFs’ priorities are the same, the LVF with a greater device MAC address becomes the new AVF.

A VF always operates in preemptive mode. When an LVF finds its priority value higher than the one advertised by the AVF, the LVF declares itself as the AVF.

VF timers

When the AVF on a router fails, the new AVF on another router creates the following timers for the failed AVF:

- **Redirect timer**—Before this timer expires, the master still uses the virtual MAC address corresponding to the failed AVF to respond to ARP/ND requests from hosts. The VF owner can share traffic load if the VF owner resumes normal operation within this time. When this timer expires, the master stops using the virtual MAC address corresponding to the failed AVF to respond to ARP/ND requests from hosts.
- **Timeout timer**—The duration after which the new AVF takes over responsibilities of the failed VF owner. Before this timer expires, all routers in the VRRP group keep the VFs that correspond to the failed AVF. The new AVF forwards packets destined for the virtual MAC address of the failed AVF. When this timer expires, all routers in the VRRP group remove the VFs that correspond to the failed AVF, including the new AVF. Packets destined for the virtual MAC address of the failed AVF are not forwarded any longer.
VF tracking

An AVF forwards packets destined for the MAC address of the AVF. If the AVF’s upstream link fails but no LVF takes over, the hosts that use the AVF’s MAC address as their gateway MAC address cannot access the external network.

The VF tracking function can solve this problem. You can use NQA or BFD to monitor the upstream link state of the VF owner, and associate the VFs with NQA or BFD through the tracking function. This enables the collaboration between VRRP and NQA or BFD through the Track module. When the upstream link fails, the state of the track entry changes to Negative. The weights of the VFs (including the AVF) on the router decrease by a specific value. The corresponding LVF with a higher priority on another router becomes the AVF and forwards packets.

Protocols and standards

- RFC 3768, Virtual Router Redundancy Protocol (VRRP)
- RFC 5798, Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6

Configuring IPv4 VRRP

VRRP cannot be configured on member ports of aggregation groups.

IPv4 VRRP configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(Required.)</em> Specifying an IPv4 VRRP operating mode</td>
<td>N/A</td>
</tr>
<tr>
<td><em>(Optional.)</em> Specifying the IPv4 VRRP version</td>
<td>N/A</td>
</tr>
<tr>
<td><em>(Required.)</em> Creating a VRRP group and assigning a virtual IP address</td>
<td>N/A</td>
</tr>
<tr>
<td><em>(Optional.)</em> Configuring the router priority, preemptive mode, and tracking function</td>
<td>N/A</td>
</tr>
<tr>
<td><em>(Optional.)</em> Configuring IPv4 VRRP packet attributes</td>
<td>N/A</td>
</tr>
<tr>
<td><em>(Optional.)</em> Configuring VF tracking</td>
<td>This configuration applies only to VRRP load balancing mode.</td>
</tr>
<tr>
<td><em>(Optional.)</em> Setting the packet sending mode for IPv4 VRRPv3</td>
<td>N/A</td>
</tr>
<tr>
<td><em>(Optional.)</em> Enabling periodic sending of gratuitous ARP packets for IPv4 VRRP</td>
<td>N/A</td>
</tr>
<tr>
<td><em>(Optional.)</em> Configuring a subordinate IPv4 VRRP group to follow a master IPv4 VRRP group</td>
<td>N/A</td>
</tr>
<tr>
<td><em>(Optional.)</em> Enabling SNMP notifications for VRRP</td>
<td>N/A</td>
</tr>
<tr>
<td><em>(Optional.)</em> Disabling an IPv4 VRRP group</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Specifying an IPv4 VRRP operating mode

A VRRP group can operate in either of the following modes:

- **Standard mode**—Only the master can forward packets.
- **Load balancing mode**—All members that have an AVF can forward packets.
After an IPv4 VRRP operating mode is configured on a router, all IPv4 VRRP groups on the router operate in the specified operating mode.

To specify an IPv4 VRRP operating mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2. Specify an IPv4 VRRP operating mode. | • Specify the standard mode: undo vrrp mode  
• Specify the load balancing mode: vrrp mode load-balance [ version-8 ] | By default, VRRP operates in standard mode. |

Specifying the IPv4 VRRP version

The VRRP version on all routers in an IPv4 VRRP group must be the same.

To specify the version of IPv4 VRRP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Specify the version of VRRP.</td>
<td>vrrp version version-number</td>
<td>By default, VRRPv3 is used.</td>
</tr>
</tbody>
</table>

Creating a VRRP group and assigning a virtual IP address

A VRRP group can operate correctly after you create it and assign a minimum of one virtual IP address to it. You can configure multiple virtual IP addresses for the VRRP group on an interface that connects to multiple subnets for router backup on different subnets.

Configuration guidelines

- Do not create a VRRP group on the VLAN interface of a super VLAN because network performance might be adversely affected. For information about the super VLAN feature, see Layer 2—LAN Switching Configuration Guide.
- A device can have a maximum of 256 VRRP groups. A VRRP group can have a maximum of 16 virtual IP addresses.
- In VRRP load balancing mode, the device supports a maximum of \textit{MaxVRNum}/N VRRP groups. \textit{MaxVRNum} refers to the maximum number of VRRP groups supported by the device in VRRP standard mode. \textit{N} refers to the number of devices in the VRRP group.
- When VRRP is operating in standard mode, the virtual IP address of a VRRP group can be either of the following addresses:
  - Unused IP address on the subnet where the VRRP group resides.
  - IP address of an interface on a router in the VRRP group.
- In load balancing mode, the virtual IP address of a VRRP group can be any unassigned IP address of the subnet where the VRRP group resides. It cannot be the IP address of any interface in the VRRP group. No IP address owner can exist in a VRRP group.
- On an IP address owner, as a best practice, do not use the \texttt{network} command to enable OSPF on the interface owning the virtual IP address of the VRRP group. For more information about the \texttt{network} command, see Layer 3—IP Routing Command Reference.
• If you create an IPv4 VRRP group without assigning virtual IP address to it, the VRRP group stays in inactive state and does not function.

• Removal of the VRRP group on the IP address owner causes IP address collision. To avoid the collision, change the IP address of the interface on the IP address owner before you remove the VRRP group from the interface.

• The virtual IP address of an IPv4 VRRP group and the downlink interface IP address of the VRRP group must be in the same subnet. Otherwise, the hosts in the subnet might fail to access external networks.

**Configuration procedure**

To create a VRRP group and assign a virtual IP address:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>vrrp vrid virtual-router-id virtual-ip virtual-address</td>
<td>By default, no VRRP groups exist.</td>
</tr>
</tbody>
</table>

**Configuring the router priority, preemptive mode, and tracking function**

The router priority determines which router in the VRRP group acts as the master. The preemptive mode enables a backup to take over as the master when it detects that it has a higher priority than the current master. The tracking function decreases the router priority or enables the backup to take over as the master when the state of the monitored track entry transits to Negative.

**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 the `vrrp vrid track priority reduced` or `vrrp vrid track switchover` command on an IP address owner, the configuration does not take effect until the router becomes a non-IP address owner.

**Configuration procedure**

To configure the router priority, preemptive mode, and tracking function:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>vrrp vrid virtual-router-id priority virtual-address</td>
<td>The default setting is 100.</td>
</tr>
<tr>
<td>4.</td>
<td>vrrp vrid virtual-router-id preempt-mode [ delay delay-value ]</td>
<td>By default, the router in a VRRP group operates in preemptive mode and the preemption delay time is 0 centiseconds, which means an immediate preemption.</td>
</tr>
</tbody>
</table>
## Configuring IPv4 VRRP packet attributes

### Configuration guidelines

- You can configure different authentication modes and authentication keys for VRRP groups on an interface. However, members of the same VRRP group must use the same authentication mode and authentication key.
- In VRRPv2, all routers in a VRRP group must have the same VRRP advertisement interval.
- In VRRPv3, authentication mode and authentication key settings do not take effect.
- In VRRPv3, routers in an IPv4 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at specified intervals, and carries the interval in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive a VRRP advertisement before the timer (3 x recorded interval + Skew_Time) expires, it regards the master as failed and takes over.

### Configuration procedure

To configure VRRP packet attributes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the authentication mode and authentication key for an IPv4 VRRP group to send and receive VRRP packets.</td>
<td>vrrp vrid virtual-router-id authentication-mode { md5</td>
</tr>
<tr>
<td>4.</td>
<td>Set the interval at which the master in an IPv4 VRRP group sends VRRP advertisements.</td>
<td>vrrp vrid virtual-router-id timer advertise adver-interval</td>
</tr>
<tr>
<td>5.</td>
<td>Specify the source interface for receiving and sending VRRP packets.</td>
<td>vrrp vrid virtual-router-id source-interface interface-type interface-number</td>
</tr>
<tr>
<td>6.</td>
<td>Enable TTL check for IPv4 VRRP packets.</td>
<td>vrrp check-ttl enable</td>
</tr>
<tr>
<td>7.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
</tbody>
</table>
8. Set a DSCP value for VRRP packets.
   vrrp dscp dscp-value
   The DSCP value identifies the packet priority during transmission.
   By default, the DSCP value for VRRP packets is 48.

### Configuring VF tracking

You can configure VF tracking in both standard mode and load balancing mode, but the function takes effect only in load balancing mode.

In load balancing mode, you can establish the collaboration between the VFs and NQA or BFD through the tracking function. When the state of the track entry transits to Negative, the weights of all VFs in the VRRP group on the router decrease by a specific value. When the state of the track entry transits to Positive or Notready, the original weight values of the VFs restore.

**Configuration guidelines**

- By default, the weight of a VF is 255, and its lower limit of failure is 10.
- When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255. The priority does not change with the weight. When the upstream link of the VF owner fails, an LVF must take over as the AVF. The switchover happens when the weight of the VF owner drops below the lower limit of failure. This requires that the reduced weight for the VF owner be higher than 245.

**Configuration procedure**

To configure VF tracking:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>vrrp vrid virtual-router-id track track-entry-number { forwarder-switchover member-ip ip-address</td>
<td>priority reduced [ priority-reduced ]</td>
</tr>
</tbody>
</table>

### Setting the packet sending mode for IPv4 VRRPv3

A router configured with VRRPv3 can process incoming VRRPv2 packets, but a router configured with VRRPv2 cannot process incoming VRRPv3 packets. When the VRRP version of the routers in a VRRP group is changed from VRRPv2 to VRRPv3, multiple masters might be elected in the VRRP group. To resolve the problem, you can set the packet sending mode for IPv4 VRRPv3. This task enables a router configured with VRRPv3 to send VRRPv2 packets and communicate with routers configured with VRRPv2.

When you set the packet sending mode for IPv4 VRRPv3, follow these restrictions and guidelines:

- The packet sending mode for IPv4 VRRPv3 takes effect only on outgoing VRRP packets. A router configured with VRRPv3 can process incoming VRRPv2 and VRRPv3 packets.
• If you set the packet sending mode for IPv4 VRRPv3 and configure VRRP packet authentication, authentication information will be carried in outgoing VRRPv2 packets but not in outgoing VRRPv3 packets.

• The VRRP advertisement interval is set in centiseconds by using the `vrrp vrid timer advertise` command. The VRRP advertisement interval carried in VRRPv2 packets sent from routers configured with VRRPv3 might be different from the configured value. For information about the VRRP advertisement interval, see the `vrrp vrid timer advertise` command in High Availability Command Reference.

To set the packet sending mode for IPv4 VRRPv3:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Set the packet sending mode for IPv4 VRRPv3.</td>
<td>`vrrp vrid virtual-router-id vrrpv3-send-packet { v2-only</td>
</tr>
</tbody>
</table>

Enabling periodic sending of gratuitous ARP packets for IPv4 VRRP

This feature enables the master router in a VRRP group to periodically send gratuitous ARP packets. Then the downstream devices can update the MAC address entry for the virtual MAC address of the VRRP group in a timely manner.

When you enable periodic sending of gratuitous ARP packets for IPv4 VRRP, follow these restrictions and guidelines:

• This feature takes effect only in VRRP standard mode.

• If you change the sending interval for gratuitous ARP packets, the configuration takes effect at the next sending interval.

• The master sends the first gratuitous ARP packet at a random time in the second half of the set interval after you execute the `vrrp send-gratuitous-arp` command. This prevents too many gratuitous ARP packets from being sent at the same time.

• The sending interval for gratuitous ARP packets might be much longer than the set interval when the following conditions are met:
  • Multiple VRRP groups exist on the device.
  • A short sending interval is set.

To enable periodic sending of gratuitous ARP packets for IPv4 VRRP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable periodic sending of gratuitous ARP packets for IPv4 VRRP.</td>
<td><code>vrrp send-gratuitous-arp [ interval interval ]</code></td>
</tr>
</tbody>
</table>
Configuring a subordinate IPv4 VRRP group to follow a master IPv4 VRRP group

Each VRRP group determines the device role (master or backup) by exchanging VRRP packets among member devices, which might consume excessive bandwidth and CPU resources. To reduce the number of VRRP packets in the network, you can configure a subordinate VRRP group to follow a master VRRP group.

A master VRRP group determines the device role through exchanging VRRP packets among member devices. A VRRP group that follows a master group, called a subordinate VRRP group, does not exchange VRRP packets among its member devices. The state of the subordinate VRRP group follows the state of the master group.

Configuration restrictions and guidelines

When you configure a subordinate IPv4 VRRP group to follow a master IPv4 VRRP group, follow these restrictions and guidelines:

- You can configure a subordinate VRRP group to follow a master VRRP group in both VRRP standard and load balancing modes. The configuration takes effect only in VRRP standard mode.
- An IPv4 VRRP group cannot be both a master group and a subordinate group.
- An IPv4 VRRP group stays in Inactive state if it is configured to follow a nonexistent master group.
- If an IPv4 VRRP group in Inactive or Initialize state follows a master group that is not in Inactive state, the state of the VRRP group does not change.
- A subordinate IPv4 VRRP group does not exchange VRRP packets, which might cause the MAC address entry for its virtual MAC address not to be updated on downstream devices. As a best practice, enable periodic sending of gratuitous ARP packets for IPv4 VRRP by using the vrrp send-gratuitous-arp command.

Configuration procedure

To configure a master IPv4 VRRP group:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>vrrp vrid virtual-router-id name name</td>
<td>By default, an IPv4 VRRP group does not act as a master group.</td>
</tr>
</tbody>
</table>

To configure a subordinate IPv4 VRRP group to follow a master IPv4 VRRP group:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>vrrp vrid virtual-router-id follow name</td>
<td>By default, an IPv4 VRRP group does not follow a master VRRP group.</td>
</tr>
</tbody>
</table>
Enabling SNMP notifications for VRRP

To report critical VRRP events to an NMS, enable SNMP notifications for VRRP. For VRRP event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

To enable SNMP notifications for VRRP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable SNMP notifications for VRRP.</td>
<td>snmp-agent trap enable vrrp [ auth-failure</td>
</tr>
</tbody>
</table>

Disabling an IPv4 VRRP group

You can temporarily disable an IPv4 VRRP group. After being disabled, the VRRP group stays in initialized state, and its configurations remain unchanged. You can change the configuration of a VRRP group when the VRRP group is disabled. Your changes take effect when you enable the VRRP group again.

To disable an IPv4 VRRP group:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Disable a VRRP group.</td>
<td>vrrp vrid virtual-router-id shutdown</td>
</tr>
</tbody>
</table>

Displaying and maintaining IPv4 VRRP

Execute `display` commands in any view and the `reset` command in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display states of IPv4 VRRP groups.</td>
<td>display vrrp [ interface interface-type interface-number [ vrid virtual-router-id ] ] [ verbose ]</td>
</tr>
<tr>
<td>Display master-to-subordinate IPv4 VRRP group bindings.</td>
<td>display vrrp binding [ interface interface-type interface-number [ vrid virtual-router-id ]</td>
</tr>
<tr>
<td>Display statistics for IPv4 VRRP groups.</td>
<td>display vrrp statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ]</td>
</tr>
<tr>
<td>Clear statistics for IPv4 VRRP groups.</td>
<td>reset vrrp statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ]</td>
</tr>
</tbody>
</table>

Configuring IPv6 VRRP

This section describes how to configure IPv6 VRRP.
IPv6 VRRP configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Specifying an IPv6 VRRP operating mode</td>
<td>N/A</td>
</tr>
<tr>
<td>(Required.) Creating a VRRP group and assigning a virtual IPv6 address</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Configuring the router priority, preemptive mode, and tracking function</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Configuring VF tracking</td>
<td>This configuration applies only to VRRP load balancing mode.</td>
</tr>
<tr>
<td>(Optional.) Configuring IPv6 VRRP packet attributes</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Enabling periodic sending of ND packets for IPv6 VRRP</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Configuring a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Disabling an IPv6 VRRP group</td>
<td>N/A</td>
</tr>
</tbody>
</table>

 Specifying an IPv6 VRRP operating mode

A VRRP group can operate in either of the following modes:

- **Standard mode**—Only the master can forward packets.
- **Load balancing mode**—All members that have an AVF can forward packets.

After the IPv6 VRRP operating mode is specified on a router, all IPv6 VRRP groups on the router operate in the specified operating mode.

To specify an IPv6 VRRP operating mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Specify an IPv6 VRRP operating mode.</td>
<td>Specify the standard mode: undo vrrp ipv6 mode. Specify the load balancing mode: vrrp ipv6 mode load-balance</td>
</tr>
</tbody>
</table>

 Creating a VRRP group and assigning a virtual IPv6 address

A VRRP group can work correctly after you create it and assign a minimum of one virtual IPv6 address for it. You can configure multiple virtual IPv6 addresses for the VRRP group on an interface that connects to multiple subnets for router backup.

**Configuration guidelines**

- Do not create VRRP groups in the VLAN interface of a super VLAN. Otherwise, network performance might be adversely affected.
- On an IP address owner, as a best practice, do not use the ospfv3 area command to enable OSPF on the interface owning the virtual IPv6 address of the VRRP group. For more information about the ospfv3 area command, see Layer 3—IP Routing Command Reference.
- 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.
- A device can have a maximum of 256 IPv6 VRRP groups. A VRRP group can have a maximum of 16 virtual IPv6 addresses.
- In VRRP load balancing mode, the device supports a maximum of $MaxVRNum/N$ VRRP groups. $MaxVRNum$ refers to the maximum number of VRRP groups supported by the device in VRRP standard mode. $N$ refers to the number of devices in the VRRP group.
- If you create an IPv6 VRRP group without assigning virtual IPv6 address to it, the VRRP group stays in inactive state and does not function.
- Removal of the VRRP group on the IP address owner causes IP address collision. To avoid the collision, change the IPv6 address of the interface on the IP address owner before you remove the VRRP group from the interface.
- The virtual IPv6 address of an IPv6 VRRP group and the downlink interface IPv6 address of the VRRP group must be in the same subnet. Otherwise, the hosts in the subnet might fail to access external networks.

### Configuration procedure

To create a VRRP group and assign a virtual IPv6 address:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>vrrp ipv6 vrid virtual-router-id virtual-ip virtual-address link-local</td>
<td>By default, no VRRP groups exist. The first virtual IPv6 address that you assign to an IPv6 VRRP group must be a link-local address. It must be the last address you remove. Only one link local address is allowed in a VRRP group.</td>
</tr>
<tr>
<td>4.</td>
<td>vrrp ipv6 vrid virtual-router-id virtual-ip virtual-address</td>
<td>By default, no global unicast address is assigned for an IPv6 VRRP group.</td>
</tr>
</tbody>
</table>

### Configuring the 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 the `vrrp ipv6 vrid track priority reduced` or `vrrp ipv6 vrid track switchover` command on an IP address owner, the configuration does not take effect until the router becomes a non-IP address owner.
- When the track entry changes from Negative to Positive or Notready, the router automatically restores its priority or the failed master router becomes the master again.

#### Configuration procedure

To configure the router priority, preemptive mode, and tracking function:
### Configuring VF tracking

You can configure VF tracking in both standard mode and load balancing mode, but the function takes effect only in load balancing mode.

In load balancing mode, you can configure the VFs in a VRRP group to monitor a track entry. When the state of the track entry transits to Negative, the weights of all VFs in the VRRP group on the router decrease by a specific value. When the state of the track entry transits to Positive or Notready, the original weights of the VFs restore.

#### Configuration guidelines

- By default, the weight of a VF is 255, and its lower limit of failure is 10.
- When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255. The priority does not change with the weight. When the upstream link of the VF owner fails, an LVF must take over as the AVF. The switchover happens when the weight of the VF owner drops below the lower limit of failure. This requires that the reduced weight for the VF owner be higher than 245.

#### Configuration procedure

To configure VF tracking:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>vrrp ipv6 vrid virtual-router-id track track-entry-number { forwarder-switchover member-ip ipv6-address</td>
<td>priority reduced</td>
</tr>
</tbody>
</table>
Configuring IPv6 VRRP packet attributes

This section describes how to configure IPv6 VRRP packet attributes.

Configuration guidelines

- The routers in an IPv6 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at the specified interval and carries the interval attribute in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive a VRRP advertisement before the timer (3 x recorded interval + Skew_Time) expires, it regards the master as failed and takes over.

- A high volume of network traffic might cause a backup to fail to receive VRRP advertisements from the master within the specified time. As a result, an unexpected master switchover occurs. To solve this problem, configure a larger interval.

Configuration procedure

To configure the IPv6 VRRP packet attribute:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 3.   | vrrp ipv6 vrid virtual-router-id timer advertise advertise-interval | The default setting is 100 centiseconds.  
As a best practice to maintain system stability, set the VRRP advertisement interval to be greater than 100 centiseconds. |
| 4.   | quit | N/A |
| 5.   | vrrp ipv6 dscp dscp-value | The DSCP value identifies the packet priority during transmission.  
By default, the DSCP value for IPv6 VRRP packets is 56. |

Enabling periodic sending of ND packets for IPv6 VRRP

This feature enables the master router in an IPv6 VRRP group to periodically send ND packets. Then the downstream devices can update the MAC address entry for the virtual MAC address of the IPv6 VRRP group in a timely manner.

When you enable periodic sending of ND packets for IPv6 VRRP, follow these restrictions and guidelines:

- This feature takes effect only in VRRP standard mode.
- If you change the sending interval for ND packets, the configuration takes effect at the next sending interval.
- The master sends the first ND packet at a random time in the second half of the set interval after you execute the vrrp ipv6 send-nd command. This prevents too many ND packets from being sent at the same time.
- The sending interval for ND packets might be much longer than the set interval when the following conditions are met:
Multiple IPv6 VRRP groups exist on the device.
A short sending interval is set.

To enable periodic sending of ND packets for IPv6 VRRP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable periodic sending of ND packets for IPv6 VRRP.</td>
<td>vrrp ipv6 send-nd [ interval interval ]</td>
</tr>
</tbody>
</table>

Configuring a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group

Each IPv6 VRRP group determines the device role (master or backup) by exchanging VRRP packets among member devices, which might consume excessive bandwidth and CPU resources. To reduce the number of VRRP packets in the network, you can configure a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group.

A master IPv6 VRRP group determines the device role through exchanging VRRP packets among member devices. An IPv6 VRRP group that follows a master group, called a subordinate VRRP group, does not exchange VRRP packets among its member devices. The state of the subordinate VRRP group follows the state of the master group.

Configuration restrictions and guidelines

When you configure a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group, follow these restrictions and guidelines:

- You can configure a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group in both VRRP standard and load balancing modes. The configuration takes effect only in VRRP standard mode.
- An IPv6 VRRP group cannot be both a master group and a subordinate group.
- An IPv6 VRRP group stays in Inactive state if it is configured to follow a nonexistent master IPv6 VRRP group.
- If an IPv6 VRRP group in Inactive or Initialize state follows a master group that is not in Inactive state, the state of the VRRP group does not change.
- A subordinate IPv6 VRRP group does not exchange VRRP packets, which might cause the MAC address entry for its virtual MAC address not to be updated on downstream devices. As a best practice, enable periodic sending of ND packets for IPv6 VRRP by using the vrrp ipv6 send-nd command.

Configuration procedure

To configure a master IPv6 VRRP group:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure an IPv6 VRRP group as a master group and assign a name to it.</td>
<td>vrrp ipv6 vrid virtual-router-id name name</td>
</tr>
</tbody>
</table>
To configure a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Configure an IPv6 VRRP group to follow a master group.</td>
<td>By default, an IPv6 VRRP group does not follow a master VRRP group.</td>
</tr>
</tbody>
</table>

Disabling an IPv6 VRRP group

You can temporarily disable an IPv6 VRRP group. After being disabled, the VRRP group stays in initialized state, and its configurations remain unchanged. You can change the configuration of a VRRP group when it is disabled. Your changes take effect when you enable the VRRP group again.

To disable an IPv6 VRRP group:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Disable an IPv6 VRRP group.</td>
<td>By default, an IPv6 VRRP group is enabled.</td>
</tr>
</tbody>
</table>

Displaying and maintaining IPv6 VRRP

Execute `display` commands in any view and the `reset` command in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the states of IPv6 VRRP groups.</td>
<td><code>display vrrp ipv6 [ interface interface-type interface-number [ vrid virtual-router-id ] ] [ verbose ]</code></td>
</tr>
<tr>
<td>Display master-to-subordinate IPv6 VRRP group bindings.</td>
<td>`display vrrp ipv6 binding [ interface interface-type interface-number [ vrid virtual-router-id ]</td>
</tr>
<tr>
<td>Display statistics for IPv6 VRRP groups.</td>
<td><code>display vrrp ipv6 statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ]</code></td>
</tr>
<tr>
<td>Clear statistics for IPv6 VRRP groups.</td>
<td><code>reset vrrp ipv6 statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ]</code></td>
</tr>
</tbody>
</table>

IPv4 VRRP configuration examples

Single VRRP group configuration example

**Network requirements**

As shown in Figure 51, Switch A and Switch B form a VRRP group. They use the virtual IP address 10.1.1.111/24 to provide gateway service for the subnet where Host A resides.
Switch A operates as the master to forward packets from Host A to Host B. When Switch A fails, Switch B takes over to forward packets for Host A.

Figure 51 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 10.1.1.1/24
   
   # Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 10.1.1.111.
   
   [SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.111
   
   # Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.
   
   [SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
   
   # Configure Switch A to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5000 centiseconds to avoid frequent status switchover.
   
   [SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000

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 10.1.1.2/24
   
   # Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 10.1.1.111.
   
   [SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.111
   
   # Set the priority of Router B to 100 in VRRP group 1.
   
   [SwitchB-Vlan-interface2] vrrp vrid 1 priority 100
# Configure Switch B to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
```

Verifying the configuration

# Ping Host B from Host A. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode     : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
   VRID       : 1                Adver Timer : 100
   Admin Status : Up             State : Master
   Config Pri   : 110             Running Pri : 110
   Preempt Mode : Yes             Delay Time : 5000
   Auth Type    : None
   Virtual IP   : 10.1.1.111
   Virtual MAC  : 0000-5e00-0101
   Master IP    : 10.1.1.1
```

# Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode     : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
   VRID       : 1                Adver Timer : 100
   Admin Status : Up             State : Backup
   Config Pri   : 100             Running Pri : 100
   Preempt Mode : Yes             Delay Time : 5000
   Become Master : 401ms left
   Auth Type    : None
   Virtual IP   : 10.1.1.111
   Master IP    : 10.1.1.1
```

The output shows that Switch A is operating as the master in VRRP group 1 to forward packets from Host A to Host B.

# Disconnect the link between Host A and Switch A, and verify that Host A can still ping Host B. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode     : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
   VRID       : 1                Adver Timer : 100
   Admin Status : Up             State : Master
   Config Pri   : 100             Running Pri : 100
   Preempt Mode : Yes             Delay Time : 5000
```
Auth Type : None
Virtual IP : 10.1.1.111
Virtual MAC : 0000-5e00-0101
Master IP : 10.1.1.2

The output shows that when Switch A fails, Switch B takes over to forward packets from Host A to Host B.

# Recover the link between Host A and Switch A, and display detailed information about VRRP group 1 on Switch A.

[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode : Standard
  Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID : 1                  Adver Timer : 100
    Admin Status : Up           State : Master
    Config Pri : 110             Running Pri : 110
    Preempt Mode : Yes           Delay Time : 5000
    Auth Type : None
    Virtual IP : 10.1.1.111
    Virtual MAC : 0000-5e00-0101
    Master IP : 10.1.1.1

The output shows that after Switch A resumes normal operation, it becomes the master to forward packets from Host A to Host B.

Multiple VRRP groups configuration example

Network requirements

As shown in Figure 52, Switch A and Switch B form two VRRP groups. VRRP group 1 uses the virtual IP address 10.1.1.100/25 to provide gateway service for hosts in VLAN 2, and VRRP group 2 uses the virtual IP address 10.1.1.200/25 to provide gateway service for hosts in VLAN 3.

Assign a higher priority to Switch A than Switch B in VRRP group 1, but a lower priority in VRRP group 2. Traffic from VLAN 2 and VLAN 3 can then be distributed between the two switches. When one of the switches fails, the healthy switch provides gateway service for both VLANs.
**Figure 52 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 10.1.1.1/25
   # Create VRRP group 1, and set its virtual IP address to 10.1.1.100.
   [SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.100
   # Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master in the group.
   [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 10.1.1.130/25
   # Create VRRP group 2, and set its virtual IP address to 10.1.1.200.
   [SwitchA-Vlan-interface3] vrrp vrid 2 virtual-ip 10.1.1.200
   ```

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 10.1.1.2/25
   ```
# Create VRRP group 1, and set its virtual IP address to 10.1.1.100.
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.100
[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 10.1.1.131 255.255.255.128

# Create VRRP group 2, and set its virtual IP address to 10.1.1.200.
[SwitchB-Vlan-interface3] vrrp vrid 2 virtual-ip 10.1.1.200

# Assign Switch B a higher priority than Switch A in VRRP group 2, so Switch B can become the master in the group.
[SwitchB-Vlan-interface3] vrrp vrid 2 priority 110

Verifying the configuration

# Display detailed information about the VRRP groups on Switch A.
[SwitchA-Vlan-interface3] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode : Standard
Total number of virtual routers : 2
Interface Vlan-interface2
  VRID : 1  Adver Timer : 100
  Admin Status : Up  State : Master
  Config Pri : 110  Running Pri : 110
  Preempt Mode : Yes  Delay Time : 0
  Auth Type : None
  Virtual IP : 10.1.1.100
  Virtual MAC : 0000-5e00-0101
  Master IP : 10.1.1.1

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 : 203ms left
  Auth Type : None
  Virtual IP : 10.1.1.200
  Master IP : 10.1.1.131

# Display detailed information about the VRRP groups on Switch B.
[SwitchB-Vlan-interface3] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode : Standard
Total number of virtual routers : 2
Interface Vlan-interface2
  VRID : 1  Adver Timer : 100
  Admin Status : Up  State : Backup
  Config Pri : 100  Running Pri : 100

Interface Vlan-interface3
  VRID : 2  Adver Timer : 100
  Admin Status : Up  State : Backup
  Config Pri : 100  Running Pri : 100
The output shows the following information:

- Switch A is operating as the master in VRRP group 1 to forward Internet traffic for hosts that use the default gateway 10.1.1.100/25.
- Switch B is operating as the master in VRRP group 2 to forward Internet traffic for hosts that use the default gateway 10.1.1.200/25.

VRRP load balancing configuration example

Network requirements

As shown in Figure 53, Switch A, Switch B, and Switch C form a load-balanced VRRP group. They use the virtual IP address 10.1.1.1/24 to provide gateway service for subnet 10.1.1.0/24.

Configure VFs on Switch A, Switch B, and Switch C to monitor their respective VLAN-interface 3. When the interface on any one of them fails, the weights of the VFs on the problematic switch decrease so another AVF can take over.
### 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 set its virtual IP address to 10.1.1.1.
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ip address 10.1.1.2 24
   [SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
   # Assign Switch A the highest priority in VRRP group 1, so Switch A can become the master.
   [SwitchA-Vlan-interface2] vrrp vrid 1 priority 120
   # Configure Switch A to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5000 centiseconds to avoid frequent status switchover.
   [SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
   [SwitchA-Vlan-interface2] quit
   # Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.
   [SwitchA] track 1 interface vlan-interface 3
   # Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.
   ```
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 set its virtual IP address to 10.1.1.1.
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] ip address 10.1.1.3 24
   [SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1

   # Assign Switch B a higher priority than Switch C in VRRP group 1, so Switch B can become the master when Switch A fails.
   [SwitchB-Vlan-interface2] vrrp vrid 1 priority 110

   # Configure Switch B to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.
   [SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
   [SwitchB-Vlan-interface2] quit

   # Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.
   [SwitchB] track 1 interface vlan-interface 3

   # Configure the VF in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] vrrp vrid 1 track 1 weight 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 set its virtual IP address to 10.1.1.1.
   [SwitchC] interface vlan-interface 2
   [SwitchC-Vlan-interface2] ip address 10.1.1.4 24
   [SwitchC-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1

   # Configure Switch C to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.
   [SwitchC-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
   [SwitchC-Vlan-interface2] quit

   # Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.
   [SwitchC] track 1 interface vlan-interface 3

205
# Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

```plaintext
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] vrrp vrid 1 track 1 weight reduced 250
```

Verifying the configuration

# Verify that Host A can ping the external network. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.

```plaintext
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode : Load Balance
  Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID           : 1                    Adver Timer  : 100
    Admin Status   : Up                   State        : Master
    Config Pri     : 120                  Running Pri  : 120
    Preempt Mode   : Yes                  Delay Time   : 5000
    Auth Type      : None
    Virtual IP     : 10.1.1.1
    Member IP List : 10.1.1.2 (Local, Master)
                      10.1.1.3 (Backup)
                      10.1.1.4 (Backup)
  Forwarder Information: 3 Forwarders 1 Active
    Config Weight  : 255
    Running Weight : 255
    Forwarder 01
      State          : Active
      Virtual MAC    : 000f-e2ff-0011 (Owner)
      Owner ID       : 0000-5e01-1101
      Priority       : 255
      Active         : local
    Forwarder 02
      State          : Listening
      Virtual MAC    : 000f-e2ff-0012 (Learnt)
      Owner ID       : 0000-5e01-1103
      Priority       : 127
      Active         : 10.1.1.3
    Forwarder 03
      State          : Listening
      Virtual MAC    : 000f-e2ff-0013 (Learnt)
      Owner ID       : 0000-5e01-1105
      Priority       : 127
      Active         : 10.1.1.4
    Forwarder Weight Track Information:
      Track Object   : 1          State : Positive  Weight Reduced : 250
```

# Display detailed information about VRRP group 1 on Switch B.

```plaintext
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode : Load Balance
```
Total number of virtual routers : 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vlan-interface2</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRID</td>
<td>1</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Up</td>
</tr>
<tr>
<td>Config Pri</td>
<td>110</td>
</tr>
<tr>
<td>Preempt Mode</td>
<td>Yes</td>
</tr>
<tr>
<td>Become Master</td>
<td>410ms left</td>
</tr>
<tr>
<td>Auth Type</td>
<td>None</td>
</tr>
<tr>
<td>Virtual IP</td>
<td>10.1.1.1</td>
</tr>
<tr>
<td>Member IP List</td>
<td>10.1.1.3 (Local, Backup)</td>
</tr>
<tr>
<td></td>
<td>10.1.1.2 (Master)</td>
</tr>
<tr>
<td></td>
<td>10.1.1.4 (Backup)</td>
</tr>
</tbody>
</table>

Forwarder Information: 3 Forwarders 1 Active

| Config Weight | 255 |
| Running Weight | 255 |

Forwarder 01

<table>
<thead>
<tr>
<th>State</th>
<th>Listening</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual MAC</td>
<td>000f-e2ff-0011 (Learnt)</td>
</tr>
<tr>
<td>Owner ID</td>
<td>0000-5e01-1101</td>
</tr>
<tr>
<td>Priority</td>
<td>127</td>
</tr>
<tr>
<td>Active</td>
<td>10.1.1.2</td>
</tr>
</tbody>
</table>

Forwarder 02

<table>
<thead>
<tr>
<th>State</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual MAC</td>
<td>000f-e2ff-0012 (Owner)</td>
</tr>
<tr>
<td>Owner ID</td>
<td>0000-5e01-1103</td>
</tr>
<tr>
<td>Priority</td>
<td>255</td>
</tr>
<tr>
<td>Active</td>
<td>local</td>
</tr>
</tbody>
</table>

Forwarder 03

<table>
<thead>
<tr>
<th>State</th>
<th>Listening</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual MAC</td>
<td>000f-e2ff-0013 (Learnt)</td>
</tr>
<tr>
<td>Owner ID</td>
<td>0000-5e01-1105</td>
</tr>
<tr>
<td>Priority</td>
<td>127</td>
</tr>
<tr>
<td>Active</td>
<td>10.1.1.4</td>
</tr>
</tbody>
</table>

Forwarder Weight Track Information:

| Track Object | 1 | State: Positive | Weight Reduced: 250 |

# Display detailed information about VRRP group 1 on Switch C.

```bash
[SwitchC-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode: Load Balance
Total number of virtual routers: 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vlan-interface2</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRID</td>
<td>1</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Up</td>
</tr>
<tr>
<td>Config Pri</td>
<td>100</td>
</tr>
<tr>
<td>Preempt Mode</td>
<td>Yes</td>
</tr>
<tr>
<td>Become Master</td>
<td>401ms left</td>
</tr>
<tr>
<td>Auth Type</td>
<td>None</td>
</tr>
<tr>
<td>Virtual IP</td>
<td>10.1.1.1</td>
</tr>
</tbody>
</table>
```
The output shows that Switch A is the master in VRRP group 1, and each of the three switches has one AVF and two LVFs.

# Disconnect the link of VLAN-interface 3 on Switch A, and display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode      : Load Balance
  Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID           : 1                  Adver Timer : 100
    Admin Status   : Up                  State : Master
    Config Pri     : 120                Running Pri : 120
    Preempt Mode   : Yes                Delay Time : 5000
    Auth Type      : None
    Virtual IP     : 10.1.1.1
    Member IP List : 10.1.1.2 (Local, Master) 10.1.1.3 (Backup) 10.1.1.4 (Backup)
Forwarder Information: 3 Forwarders 0 Active
  Config Weight : 255
  Running Weight : 5
  Forwarder 01
```
State          : Initialize
Virtual MAC    : 000f-e2ff-0011 (Owner)
Owner ID       : 0000-5e01-1101
Priority       : 0
Active         : 10.1.1.4
Forwarder 02
State          : Initialize
Virtual MAC    : 000f-e2ff-0012 (Learnt)
Owner ID       : 0000-5e01-1103
Priority       : 0
Active         : 10.1.1.3
Forwarder 03
State          : Initialize
Virtual MAC    : 000f-e2ff-0013 (Learnt)
Owner ID       : 0000-5e01-1105
Priority       : 0
Active         : 10.1.1.4
Forwarder Weight Track Information:
  Track Object   : 1          State : Negative   Weight Reduced : 250

# Display detailed information about VRRP group 1 on Switch C.

[SwitchC-Vlan-interface2] display vrrp verbose

IPv4 Virtual Router Information:
Running Mode      : Load Balance
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID           : 1                    Adver Timer  : 100
  Admin Status   : Up                   State        : Backup
  Config Pri     : 100                  Running Pri  : 100
  Preempt Mode   : Yes                  Delay Time   : 5000
  Become Master  : 401ms 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
Forwarder 02
State          : Listening
Virtual MAC    : 000f-e2ff-0012 (Learnt)
Owner ID       : 0000-5e01-1103
The output shows that when VLAN-interface 3 on Switch A fails, the weights of the VFs on Switch A drop below the lower limit of failure. All VFs on Switch A transit to the Initialized state and cannot forward traffic. The VF for MAC address 000f-e2ff-0011 on Switch C becomes the AVF to forward traffic.

# When the timeout timer (about 1800 seconds) expires, display detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
    Running Mode : Load Balance
    Total number of virtual routers : 1
    Interface Vlan-interface2
        VRID : 1          Adver Timer : 100
        Admin Status : Up       State : Backup
        Config Pri : 100        Running Pri : 100
        Preempt Mode : Yes       Delay Time : 5000
        Become Master : 402ms left
        Auth Type : None
        Virtual IP : 10.1.1.1
        Member IP List : 10.1.1.4 (Local, Backup)
                        10.1.1.2 (Master)
                        10.1.1.3 (Backup)
Forwarder Information: 2 Forwarders 1 Active
    Config Weight : 255
    Running Weight : 255
    Forwarder 02
        State : Listening
        Virtual MAC : 000f-e2ff-0012 (Learnt)
        Owner ID : 0000-5e01-1103
        Priority : 127
        Active : 10.1.1.3
    Forwarder 03
        State : Active
        Virtual MAC : 000f-e2ff-0013 (Owner)
        Owner ID : 0000-5e01-1105
        Priority : 255
        Active : local
Forwarder Weight Track Information:
    Track Object : 1          State : Positive   Weight Reduced : 250
```

The output shows that when VLAN-interface 3 on Switch A fails, the weights of the VFs on Switch A drop below the lower limit of failure. All VFs on Switch A transit to the Initialized state and cannot forward traffic. The VF for MAC address 000f-e2ff-0011 on Switch C becomes the AVF to forward traffic.
The output shows that when the timeout timer expires, the VF for virtual MAC address 000f-e2ff-0011 is removed. The VF no longer forwards the packets destined for the MAC address.

# When Switch A fails, display detailed information about VRRP group 1 on Switch B.

```bash
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode : Load Balance
  Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID : 1          Adver Timer : 100
    Admin Status : Up    State : Master
    Config Pri : 110      Running Pri : 110
    Preempt Mode : Yes     Delay Time : 5000
    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 the following information:

- When Switch A fails, Switch B becomes the master because it has a higher priority than Switch C.
- The VF for virtual MAC address 000f-e2ff-0011 is removed.

**IPv6 VRRP configuration examples**

**Single VRRP group configuration example**

**Network requirements**

As shown in Figure 54, Switch A and Switch B form a VRRP group. They use the virtual IP addresses 1::10/64 and FE80:::10 to provide gateway service for the subnet where Host A resides.

Host A learns 1::10/64 as its default gateway from RA messages sent by the switches.
Switch A operates as the master to forward packets from Host A to Host B. When Switch A fails, Switch B takes over to forward packets for Host A.

**Figure 54 Network diagram**

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] ipv6 address fe80::1 link-local
   [SwitchA-Vlan-interface2] ipv6 address 1::1 64
   
   # Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
   
   # Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
   
   # Configure Switch A to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5000 centiseconds to avoid frequent status switchover.
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000
   
   # Enable Switch A to send RA messages, so Host A can learn the default gateway address.
   [SwitchA-Vlan-interface2] undo ipv6 nd ra halt
   
   # 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] ipv6 address fe80::2 link-local
   [SwitchA-Vlan-interface2] ipv6 address 1::2 64
   ```

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] ipv6 address fe80::2 link-local
   [SwitchB-Vlan-interface2] ipv6 address 1::2 64
   ```
# Create VRRP group 1 and set its virtual IPv6 addresses to FE80::10 and 1::10.
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10

# Configure Switch B to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000

# Enable Switch B to send RA messages, so Host A can learn the default gateway address.
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt

Verifying the configuration

# Ping Host B from Host A. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
  Running Mode : Standard
  Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID : 1 Adver Timer : 100
    Admin Status : Up State : Master
    Config Pri : 110 Running Pri : 110
    Preempt Mode : Yes Delay Time : 5000
    Auth Type : None
    Virtual IP : FE80::10 1::10
    Virtual MAC : 0000-5e00-0201
    Master IP : FE80::1

# Display detailed information about VRRP group 1 on Switch B.
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
  Running Mode : Standard
  Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID : 1 Adver Timer : 100
    Admin Status : Up State : Backup
    Config Pri : 100 Running Pri : 100
    Preempt Mode : Yes Delay Time : 5000
    Become Master : 403ms left
    Auth Type : None
    Virtual IP : FE80::10 1::10
    Master IP : FE80::1

The output shows that Switch A is operating as the master in VRRP group 1 to forward packets from Host A to Host B.

# Disconnect the link between Host A and Switch A, and verify that Host A can still ping Host B. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch B.
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
Running Mode : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID           : 1          Adver Timer  : 100
  Admin Status   : Up         State : Master
  Config Pri     : 100        Running Pri : 100
  Preempt Mode   : Yes        Delay Time   : 5000
  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 takes over to forward packets from Host A to Host B.

# Recover the link between Host A and Switch A, and display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
```

IPv6 Virtual Router Information:
Running Mode : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID           : 1          Adver Timer  : 100
  Admin Status   : Up         State : Master
  Config Pri     : 110        Running Pri : 110
  Preempt Mode   : Yes        Delay Time   : 5000
  Auth Type      : None
  Virtual IP     : FE80::10
                   1::10
  Virtual MAC    : 0000-5e00-0201
  Master IP      : FE80::2

The output shows that after Switch A resumes normal operation, it becomes the master to forward packets from Host A to Host B.

Multiple VRRP groups configuration example

Network requirements

As shown in Figure 55, Switch A and Switch B form two VRRP groups. VRRP group 1 uses the virtual IPv6 addresses 1::10/64 and FE80::10 to provide gateway service for hosts in VLAN 2. VRRP group 2 uses the virtual IPv6 addresses 2::10/64 and FE90::10 to provide gateway service for hosts in VLAN 3.

From RA messages sent by the switches, hosts in VLAN 2 learn 1::10/64 as their default gateway. Hosts in VLAN 3 learn 2::10/64 as their default gateway.

Assign Switch A a higher priority than Switch B in VRRP group 1 but a lower priority in VRRP group 2. Traffic from VLAN 2 and VLAN 3 can then be distributed between the two switches. When one of the switches fails, the healthy switch provides gateway service for both VLANs.
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] 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
   # Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master in the group.
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
   # Enable Switch A to send RA messages, so hosts in VLAN 2 can learn the default gateway address.
   [SwitchA-Vlan-interface2] undo ipv6 nd ra halt
   [SwitchA-Vlan-interface2] quit

   # Configure VLAN 3.
   [SwitchA] vlan 3
   [SwitchA-vlan3] port gigabitethernet 1/0/6
   [SwitchA-vlan3] quit
   [SwitchA] interface vlan-interface 3
   [SwitchA-Vlan-interface3] ipv6 address fe90::1 link-local
   [SwitchA-Vlan-interface3] ipv6 address 2::1/64
   # Create VRRP group 2, and set its virtual 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 hosts in VLAN 3 can learn the default gateway address.
[SwitchA-Vlan-interface3] undo ipv6 nd ra halt

2. Configure Switch B:
   # Configure VLAN 2.
   <SwitchB> system-view
   [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
   # Enable Switch B to send RA messages, so hosts in VLAN 2 can learn the default gateway address.
   [SwitchB-Vlan-interface2] undo ipv6 nd ra halt
   [SwitchB-Vlan-interface2] quit
   # Configure VLAN 3.
   [SwitchB] vlan 3
   [SwitchB-vlan3] port gigabitethernet 1/0/6
   [SwitchB-vlan3] quit
   [SwitchB] interface vlan-interface 3
   [SwitchB-Vlan-interface3] ipv6 address fe90::2 link-local
   [SwitchB-Vlan-interface3] ipv6 address 2::2 64
   # Create VRRP group 2, and set its virtual 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
   # Assign Switch B a higher priority than Switch A in VRRP group 2, so Switch B can become the master in the group.
   [SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 priority 110
   # Enable Switch B to send RA messages, so hosts in VLAN 3 can learn the default gateway address.
   [SwitchB-Vlan-interface3] undo ipv6 nd ra halt

Verifying the configuration

# Display detailed information about the VRRP groups on Switch A.
[SwitchA-Vlan-interface3] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
Running Mode : Standard
Total number of virtual routers : 2
Interface Vlan-interface2
   VRID : 1                 Adver Timer : 100
   Admin Status : Up        State : Master
   Config Pri : 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
Admin Status   : Up
Config Pri     : 100
Preempt Mode   : Yes
Become Master  : 402ms left
Auth Type      : None
Virtual IP     : FE90::10
                2::10
Master IP      : FE90::2

# Display detailed information about the VRRP groups on Switch B.
[SwitchB-Vlan-interface3] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 2
Interface Vlan-interface2
VRID           : 1
Admin Status   : Up
Config Pri     : 100
Preempt Mode   : Yes
Become Master  : 401ms left
Auth Type      : None
Virtual IP     : FE80::10
                1::10
Master IP      : FE80::1

Interface Vlan-interface3
VRID           : 2
Admin Status   : Up
Config Pri     : 110
Preempt Mode   : Yes
Auth Type      : None
Virtual IP     : FE90::10
                2::10
Virtual MAC    : 0000-5e00-0202
Master IP      : FE90::2

The output shows the following information:
- Switch A is operating as the master in VRRP group 1 to forward Internet traffic for hosts that use the default gateway 1::10/64.
- Switch B is operating as the master in VRRP group 2 to forward Internet traffic for hosts that use the default gateway 2::10/64.
VRRP load balancing configuration example

Network requirements

As shown in Figure 56, Switch A, Switch B, and Switch C form a load balanced VRRP group. They use the virtual IPv6 addresses FE80::10 and 1::10 to provide gateway service for subnet 1::/64.

Hosts on subnet 1::/64 learn 1::10 as their default gateway from RA messages sent by the switches.

Configure VFIs on Switch A, Switch B, or Switch C to monitor their respective VLAN-interface 3. When the interface on any of them fails, the weights of the VFIs on the problematic switch decrease so another AVF can take over.

Figure 56 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 ipv6 mode load-balance
   # Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
   [SwitchA-Vlan-interface2] ipv6 address 1::1 64
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
# Assign Switch A the highest priority in VRRP group 1, so Switch A can become the master.
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 120

# Configure Switch A to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5000 centiseconds to avoid frequent status switchover.
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000

# Enable Switch A to send RA messages, so hosts on subnet 1::/64 can learn the default gateway address.
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
[SwitchA-Vlan-interface2] quit

# Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.
[SwitchA] track 1 interface vlan-interface 3

# Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight 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 ipv6 mode load-balance

# Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10

# Assign Switch B a higher priority than Switch C in VRRP group 1, so Switch B can become the master when Switch A fails.
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 priority 110

# Configure Switch B to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000

# Enable Switch B to send RA messages so hosts on subnet 1::/64 can learn the default gateway address.
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
[SwitchB-Vlan-interface2] quit

# Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.
[SwitchB] track 1 interface vlan-interface 3

# Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight 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 ipv6 mode load-balance

# Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ipv6 address fe80::3 link-local
[SwitchC-Vlan-interface2] ipv6 address 1::3 64
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10

# Configure Switch C to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000

# Enable Switch C to send RA messages, so the hosts on the subnet 1::/64 can learn the default gateway address.
[SwitchC-Vlan-interface2] undo ipv6 nd ra halt
[SwitchC-Vlan-interface2] quit

# Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.
[SwitchC] track 1 interface vlan-interface 3

# Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight reduced 250

Verifying the configuration

# Verify that Host A can ping the external network. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
Running Mode : Load Balance
Total number of virtual routers : 1
Interface Vlan-interface2
VRID : 1
Admin Status : Up
Config Pri : 120
Preempt Mode : Yes
Auth Type : None
Virtual IP : FE80::10
           1::10
Member IP List : FE80::1 (Local, Master)
                FE80::2 (Backup)
                FE80::3 (Backup)
Forwarder Information: 3 Forwarders 1 Active
Config Weight : 255
Running Weight : 255
Forwarder 01
State : Active
Virtual MAC : 000f-e2ff-4011 (Owner)
Owner ID : 0000-5e01-1101
Priority : 255
Active : local

Forwarder 02
State : Listening
Virtual MAC : 000f-e2ff-4012 (Learnt)
Owner ID : 0000-5e01-1103
Priority : 127
Active : FE80::2

Forwarder 03
State : Listening
Virtual MAC : 000f-e2ff-4013 (Learnt)
Owner ID : 0000-5e01-1105
Priority : 127
Active : FE80::3

Forwarder Weight Track Information:
Track Object : 1 State : Positive Weight Reduced : 250

# Display detailed information about VRRP group 1 on Switch B.
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
Running Mode : Load Balance
Total number of virtual routers : 1
Interface Vlan-interface2
   VRID : 1 Adver Timer : 100
   Admin Status : Up State : Backup
   Config Pri : 110 Running Pri : 110
   Preempt Mode : Yes Delay Time : 5000
   Become Master : 401ms left
   Auth Type : None
   Virtual IP : FE80::10
   1::10
   Member IP List : FE80::2 (Local, Backup)
                  FE80::1 (Master)
                  FE80::3 (Backup)
Forwarder Information: 3 Forwarders 1 Active
Config Weight : 255
Running Weight : 255
Forwarder 01
State : Listening
Virtual MAC : 000f-e2ff-4011 (Learnt)
Owner ID : 0000-5e01-1101
Priority : 127
Active : FE80::1

Forwarder 02
State : Active
Virtual MAC     : 000f-e2ff-4012 (Owner)
Owner ID        : 0000-5e01-1103
Priority        : 255
Active          : local

Forwarder 03

State          : Listening
Virtual MAC    : 000f-e2ff-4013 (Learnt)
Owner ID       : 0000-5e01-1105
Priority       : 127
Active         : FE80::3

Forwarder Weight Track Information:

Track Object   : 1          State : Positive   Weight Reduced : 250

# Display detailed information about VRRP group 1 on Switch C.

[SwitchC-Vlan-interface2] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode     : Load Balance
Total number of virtual routers : 1

Interface Vlan-interface2

VRID           : 1                    Adver Timer  : 100
Admin Status   : Up                   State        : Backup
Config Pri     : 100                  Running Pri  : 100
Preempt Mode   : Yes                  Delay Time   : 5000
Become Master  : 402ms 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 Switch A is the master in VRRP group 1, and each of the three switches has one AVF and two LVFs.

# Disconnect the link of VLAN-interface 3 on Switch A and display detailed information about VRRP group 1 on Switch A.

[SwitchA-Vlan-interface2] display vrrp ipv6 verbose

IPv6 Virtual Router Information:

Running Mode      : Load Balance
Total number of virtual routers : 1
Interface Vlan-interface2
VRID           : 1                    Adver Timer  : 100
Admin Status   : Up                   State        : Master
Config Pri     : 120                  Running Pri  : 120
Preempt Mode   : Yes                  Delay Time   : 5000
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

Forwarder 01
State            : Initialize
Virtual MAC  : 000f-e2ff-4011 (Owner)
Owner ID       : 0000-5e01-1101
Priority       : 0
Active         : FE80::3

Forwarder 02
State            : Initialize
Virtual MAC  : 000f-e2ff-4012 (Learnt)
Owner ID       : 0000-5e01-1103
Priority       : 0
Active         : FE80::2

Forwarder 03
State            : Initialize
Virtual MAC  : 000f-e2ff-4013 (Learnt)
Owner ID       : 0000-5e01-1105
Priority       : 0
Active         : FE80::3

Forwarder Weight Track Information:

Track Object   : 1          State : Negative   Weight Reduced : 250

# Display detailed information about VRRP group 1 on Switch C.

[SwitchC-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
Running Mode : Load Balance
Total number of virtual routers : 1
Interface Vlan-interface2
   VRID           : 1                    Adver Timer  : 100
   Admin Status   : Up                   State        : Backup
   Config Pri     : 100                  Running Pri  : 100
   Preempt Mode   : Yes                  Delay Time   : 5000
   Become Master  : 410ms 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
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 weights of the VFs on Switch A drop below the lower limit of failure. All VFs on Switch A transit to the Initialized state and cannot forward traffic. The VF for MAC address 000f-e2ff-4011 on Switch C becomes the AVF to forward traffic.

# When the timeout timer (about 1800 seconds) expires, display detailed information about VRRP group 1 on Switch C.
[SwitchC-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
   Running Mode : Load Balance
Total number of virtual routers : 1
   Interface Vlan-interface2
The output shows that when the timeout timer expires, the VF for virtual MAC address 000f-e2ff-4011 is removed. The VF no longer forwards the packets destined for the MAC address.

# When Switch A fails, display detailed information about VRRP group 1 on Switch B.

[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
  Running Mode : Load Balance
  Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID : 1                     Adver Timer : 100
    Admin Status : Up             State : Master
    Config Pri : 110               Running Pri : 110
    Preempt Mode : Yes             Delay Time : 5000
    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 : 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
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 the following information:
- When Switch A fails, Switch B becomes the master because it has a higher priority than Switch C.
- The VF for virtual MAC address 000f-e2ff-4011 is removed.

Troubleshooting VRRP

An error prompt is displayed

Symptom
An error prompt "The virtual router detected a VRRP configuration error." is displayed during configuration.

Analysis
This symptom is probably caused by the following reasons:
- The VRRP advertisement interval in the packet is not the same as that for the current VRRP group (in VRRPv2 only).
- The number of virtual IP addresses in the packet is not the same as that for the current VRRP group.
- The virtual IP address list is not the same as that for the current VRRP group.
- A device in the VRRP group receives illegitimate VRRP packets. For example, the IP address owner receives a VRRP packet with the priority 255.

Solution
To resolve the problem:
1. Modify the configuration on routers in VRRP groups to ensure consistent configuration.
2. Take fault location and anti-attack measures to eliminate potential threats.
3. If the problem persists, contact Hewlett Packard Enterprise Support.

Multiple masters appear in a VRRP group

Symptom
Multiple masters appear in a VRRP group.
Analysis

It is normal for a VRRP group to have multiple masters for a short time, and this situation requires no manual intervention.

If multiple masters coexist for a longer period, check for the following conditions:
- The masters cannot receive advertisements from each other.
- The received advertisements are illegitimate.

Solution

To resolve the problem:
1. Ping between these masters:
   - If the ping operation fails, examine network connectivity.
   - If the ping operation succeeds, check for configuration inconsistencies in the number of virtual IP addresses, virtual IP addresses, and authentication. For IPv4 VRRP, also make sure the same version of VRRP is configured on all routers in the VRRP group. For VRRPv2, make sure the same VRRP advertisement interval is configured on the routers in the VRRP group.
2. If the problem persists, contact Hewlett Packard Enterprise Support.

Fast VRRP state flapping

Symptom

Fast VRRP state flapping occurs.

Analysis

The VRRP advertisement interval is set too short.

Solution

To resolve the problem:
1. Increase the interval for sending VRRP advertisements or introduce a preemption delay.
2. If the problem persists, contact Hewlett Packard Enterprise Support.
Configuring Reth interfaces

About Reth interfaces

A redundant Ethernet (Reth) interface is a virtual Layer 3 interface that uses two member interfaces to ensure link availability. One member interface is active and the other is inactive. When the active interface fails, the inactive interface becomes active. The member interface switchover does not interrupt traffic.

NOTE:
On the device, Reth member interfaces can only be management Ethernet ports.

Applicable scenario

As shown in Figure 57, M-GigabitEthernet 1/0/0/0 and M-GigabitEthernet 1/0/0/1 are member interfaces of a Reth interface. The Reth interface selects the member interface to forward traffic as follows:

- When both member interfaces are operating correctly, the Reth interface forwards traffic through M-GigabitEthernet 1/0/0/0 and places M-GigabitEthernet 1/0/0/1 in inactive state.
- When M-GigabitEthernet 1/0/0/0 fails, M-GigabitEthernet 1/0/0/1 becomes active and the Reth interface switches traffic over to M-GigabitEthernet 1/0/0/1.

Figure 57 Reth interfaces

Operating mechanism

A member interface of a Reth interface can be in either of the following states:

- **Active**—The interface can forward packets. A Reth interface can have only one active member interface.
- **Inactive**—The interface cannot forward packets.

A Reth interface determines the state of its member interfaces by using the following rules:

- When both member interfaces are physically up, the member interface with the higher priority is active and the member interface with lower priority is inactive. The priorities of the member interfaces are user configurable.
- When the active member interface goes down physically, the inactive interface automatically becomes active to forward packets.
• When both member interfaces are physically down, both interfaces are inactive.

The Reth interface uses the device bridge MAC address as its MAC address and can be configured with an IP address. For the upstream and downstream devices, they are connected to the Reth interface. The switchover between the Reth member interfaces is not visible to the network and does not cause network topology changes.

Configuration restrictions and guidelines

To use the Reth interface features, make sure the MPUs have a minimum of two management Ethernet ports.

The IP addresses of the management Ethernet ports become invalid after you assign them to a Reth interface. To log in to the device, you must use the IP address assigned to the Reth interface.

Configuring a Reth interface

When you configure a Reth interface, follow these restrictions and guidelines:

• You can assign a maximum of two member interfaces to a Reth interface. The member interfaces must have different priorities.

• Before you delete a Reth interface, make sure all its member interfaces have been removed.

To configure a Reth interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a Reth interface and enter its view.</td>
<td>interface reth interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Assign a member interface to the Reth interface.</td>
<td>member interface interface-type interface-number priority priority</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Configure the expected bandwidth for the Reth interface.</td>
<td>bandwidth bandwidth-value</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Configure the description of the Reth interface.</td>
<td>description text</td>
</tr>
<tr>
<td>6.</td>
<td>(Optional.) Set the MTU of the Reth interface.</td>
<td>mtu size</td>
</tr>
<tr>
<td>7.</td>
<td>Bring up the Reth interface.</td>
<td>undo shutdown</td>
</tr>
<tr>
<td>8.</td>
<td>(Optional.) Restore the default settings for the Reth interface.</td>
<td>default</td>
</tr>
</tbody>
</table>

Displaying and maintaining Reth interfaces

Execute display commands in any view and reset commands in user view.
### Reth interface configuration example

#### Network requirements

As shown in **Figure 58**, configure a Reth interface as follows:

- Assign M-GigabitEthernet 1/0/0/0 and M-GigabitEthernet 1/0/0/1 to the Reth interface.
- Assign a higher priority to M-GigabitEthernet 1/0/0/0 for it to be the active member interface.

**Figure 58 Network diagram**

![Diagram showing the network setup with Reth interface](image)

#### Configuration procedure

1. Create Reth 1, and assign an IP address to the interface.
   ```
   [Sysname] interface reth 1
   [Sysname-Reth-1] ip address 1.0.0.3 24
   ```

2. Assign M-GigabitEthernet 1/0/0/0 and M-GigabitEthernet 1/0/0/1 to Reth 1, and set their priority to 100 and 80, respectively.
   ```
   [Sysname-Reth1] member interface M-GigabitEthernet1/0/0/0 priority 100
   [Sysname-Reth1] member interface M-GigabitEthernet1/0/0/1 priority 80
   ```

#### Verifying the configuration

1. Verify that M-GigabitEthernet 1/0/0/0 is active and M-GigabitEthernet 1/0/0/1 is inactive.
   ```
   [Sysname-Reth1] display reth interface reth 1
   Reth1 :
   Redundancy group : N/A
   Member         Physical status  Forwarding status  Presence status
   MGE1/0/0/0     UP            Active           Normal
   MGE1/0/0/1     Down          N/A             N/A
   ```
# Shut down M-GigabitEthernet 1/0/0/0.
[Sysname-Reth1] quit
[Sysname] interface M-GigabitEthernet 1/0/0/0
[Sysname-M-GigabitEthernet 1/0/0/0] shutdown

# Verify that M-GigabitEthernet 1/0/0/1 becomes active and M-GigabitEthernet 1/0/0/0 becomes inactive.
[Sysname-M-GigabitEthernet 1/0/0/0] display reth interface reth 1
Reth1 :
<table>
<thead>
<tr>
<th>Redundancy group</th>
<th>Physical status</th>
<th>Forwarding status</th>
<th>Presence status</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGE1/0/0/0</td>
<td>DOWN</td>
<td>Inactive</td>
<td>Normal</td>
</tr>
<tr>
<td>MGE1/0/0/1</td>
<td>UP</td>
<td>Active</td>
<td>Normal</td>
</tr>
</tbody>
</table>
Configuring BFD

Overview

Bidirectional forwarding detection (BFD) provides a general-purpose, standard, medium- and protocol-independent fast failure detection mechanism. It can detect and monitor the connectivity of links in IP to detect communication failures quickly so that measures can be taken to ensure service continuity and enhance network availability.

BFD can uniformly and quickly detect the failures of the bidirectional forwarding paths between two devices for upper-layer protocols such as routing protocols. The hello mechanism used by upper-layer protocols needs seconds to detect a link failure, while BFD can provide detection measured in milliseconds.

BFD can be used for single-hop and multihop detections.

- **Single-hop detection**—Detects the IP connectivity between two directly connected systems.
- **Multihop detection**—Detects any of the paths between two systems. These paths have multiple hops, and might overlap.

BFD session establishment and termination

Establishing a BFD session

BFD does not provide any neighbor discovery mechanisms. The upper protocol notifies BFD of the routers to which it needs to establish sessions.

A BFD session is established as follows:

1. A protocol sends Hello messages to discover neighbors and establish neighborships.
2. After establishing a neighborship, the protocol notifies BFD of the neighbor information, including destination and source addresses.
3. BFD uses the information to establish a BFD session.

Terminating a BFD session

When BFD detects a link failure, it performs the following tasks:

1. BFD clears the neighbor session.
2. BFD notifies the protocol of the failure.
3. The protocol terminates the neighborship on the link.
4. If a backup link is available, the protocol will use it for communication.

BFD session modes and operating modes

BFD sessions use the following types of packets:

- **Echo packets**—Encapsulated into UDP packets with port number 3785.
- **Control packets**—Encapsulated into UDP packets with port number 3784 for single-hop detection or port number 4784 for multihop detection.

Echo packet mode

The local end of the link sends echo packets to establish BFD sessions and monitor link status. The peer end does not establish BFD sessions and only forwards the packets back to the originating end.

In echo packet mode, BFD supports only single-hop detection and the BFD session is independent of the operating mode.
Control packet mode

Both ends of the link exchange BFD control packets to monitor link status.

Before a BFD session is established, BFD has two 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 active mode for a BFD session to be established.

After a BFD session is established, the two ends can operate in the following BFD operating modes:

- **Asynchronous mode**—The device periodically sends BFD control packets. The device considers that the session is down if it does not receive any BFD control packets within a specific interval.
- **Demand mode**—The device periodically sends BFD control packets. If the peer end is operating in Asynchronous mode (default), the peer end stops sending BFD control packets. If the peer end is operating in Demand mode, both ends stop sending BFD control packets. When the connectivity to another system needs to be verified explicitly, a system sends several BFD control packets with the Poll (P) bit set at the negotiated transmit interval. If no response is received within the detection interval, the session is considered down. If the connectivity is found to be up, no more BFD control packets are sent until the next command is issued.

In addition, both ends of the link can exchange BFD control packets to establish and maintain BFD sessions, and one end of the link sends echo packets to monitor link status.

Supported features

- Static routing. For more information, see *Layer 3—IP Routing Configuration Guide*.
- IPv6 static routing. For more information, see *Layer 3—IP Routing Configuration Guide*.
- RIP. For more information, see *Layer 3—IP Routing Configuration Guide*.
- 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*.
- 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). IP FRR is supported by BGP, 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*
• RFC 5885, Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)

Configuration restrictions and guidelines

Layer 3 aggregate interfaces/subinterfaces and Layer 3 Ethernet subinterfaces do not support BFD.

Configuring BFD basic functions

Before configuring BFD basic functions, configure the network layer addresses of the interfaces so that adjacent nodes are reachable to each other at the network layer.

After a BFD session is established, the two ends negotiate BFD parameters, including minimum sending interval, minimum receiving interval, initialization mode, and packet authentication, by exchanging negotiation packets. They use the negotiated parameters without affecting the session status.

By default, the device runs BFD version 1 and is compatible with BFD version 0. You cannot change the BFD version to 0 through commands. When the peer device runs BFD version 0, the local device automatically switches to BFD version 0.

Configuring echo packet mode

⚠ CAUTION:
To avoid echo packet loss, do not configure the echo packet mode on a device with uRPF enabled. For more information about uRPF, see Security Configuration Guide.

To configure echo packet mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the source IP address of echo packets.</td>
<td>By default, no source IP address is configured for echo packets. The source IP address cannot be on the same network segment as any local interface’s IP address. Otherwise, a large number of ICMP redirect packets might be sent from the peer, resulting in link congestion. The source IPv6 address of echo packets can only be a global unicast address.</td>
</tr>
<tr>
<td>•</td>
<td>Configure the source IP address of echo packets: bfd echo-source-ip ip-address</td>
<td></td>
</tr>
<tr>
<td>•</td>
<td>Configure the source IPv6 address of echo packets: bfd echo-source-ipv6 ipv6-address</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Set the minimum interval for receiving BFD echo packets.</td>
<td>bfd min-echo-receive-interval interval</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Set the single-hop detection time multiplier.</td>
<td>bfd detect-multiplier value</td>
</tr>
</tbody>
</table>
# Configuring control packet mode

## To configure control packet mode for single-hop detection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Specify the mode for establishing a BFD session.</td>
<td>bfd session init-mode { active</td>
</tr>
<tr>
<td>3.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the authentication mode for single-hop control packets.</td>
<td>bfd authentication-mode { m-md5</td>
</tr>
<tr>
<td>5.</td>
<td>Enable the Demand BFD session mode.</td>
<td>bfd demand enable</td>
</tr>
<tr>
<td>6.</td>
<td>Enable the echo packet mode.</td>
<td>bfd echo [ receive</td>
</tr>
<tr>
<td>7.</td>
<td>Set the minimum interval for transmitting single-hop BFD control packets.</td>
<td>bfd min-transmit-interval interval</td>
</tr>
<tr>
<td>8.</td>
<td>Set the minimum interval for receiving single-hop BFD control packets.</td>
<td>bfd min-receive-interval interval</td>
</tr>
<tr>
<td>9.</td>
<td>Set the single-hop detection time multiplier.</td>
<td>bfd detect-multiplier value</td>
</tr>
</tbody>
</table>

## To configure control packet mode for multihop detection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Specify the mode for establishing a BFD session.</td>
<td>bfd session init-mode { active</td>
</tr>
</tbody>
</table>
### Enabling SNMP notifications for BFD

To report critical BFD events to an NMS, enable SNMP notifications for BFD. For BFD event notifications to be sent correctly, you must also configure SNMP as described in *Network Management and Monitoring Configuration Guide*.

To enable SNMP notifications for BFD:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>snmp-agent trap enable bfd</td>
<td>By default, SNMP notifications are enabled for BFD.</td>
</tr>
</tbody>
</table>

### Displaying and maintaining BFD

Execute the `display` command in any view and the `reset` command in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display BFD session information.</td>
<td>`display bfd session [ discriminator value</td>
</tr>
<tr>
<td>Clear BFD session statistics.</td>
<td><code>reset bfd session statistics</code></td>
</tr>
</tbody>
</table>
Configuring Track

Overview

The Track module works between application modules and detection modules. It shields the differences between various detection modules from application modules.

Collaboration is enabled when you associate the Track module with a detection module and an application module, and it operates as follows:
1. 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.
2. The Track module sends the detection results to the application module.
3. When notified of changes for the tracked object, the application modules can react to avoid communication interruption and network performance degradation.

Collaboration fundamentals

The Track module collaborates with detection modules and application modules.

Collaboration between the Track module and a detection module

The detection module sends the detection result of the tracked object to the Track module. The Track module changes the status of the track entry as follows:
- If the tracked object operates correctly, the state of the track entry is Positive. For example, the track entry state is Positive in one of the following conditions:
  - The target interface is up.
  - The target network is reachable.
- If the tracked object does not operate correctly, the state of the track entry is Negative. For example, the track entry state is Negative in one of the following conditions:
  - The target interface is down.
  - The target network is unreachable.
- If the detection result is invalid, the state of the track entry is NotReady. For example, the track entry state is NotReady if its associated NQA operation does not exist.

The following detection modules can be associated with the Track module:
- NQA.
- BFD.
- CFD.
- Interface management.
- Route management.
- LLDP.

Collaboration between the Track module and an application module

The following application modules can be associated with the Track module:
- VRRP.
- Static routing.
- PBR.
- Smart Link.
• EVI IS-IS.
• VPLS.
• VXLAN.
• MPLS L2VPN.
• EAA.
• ERPS.

When configuring a track entry for an application module, you can set a notification delay to avoid immediate notification of status changes.

When the delay is not configured and the route convergence is slower than the link state change notification, communication failures occur. For example, when the master in a VRRP group detects an uplink interface failure through Track, Track immediately notifies the master to decrease its priority. A backup with a higher priority then preempts as the new master. When the failed uplink interface recovers, the Track module immediately notifies the original master to restore its priority. If the uplink route has not recovered, forwarding failure will occur.

Collaboration application example

The following is an example of collaboration between NQA, Track, and static routing.

Configure a static route with the 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 is invalid. For this purpose, configure NQA-Track-static routing collaboration as follows:

1. Create an NQA operation to monitor the accessibility of IP address 192.168.0.88.
2. Create a track entry and associate it with the NQA operation.
   o When the next hop 192.168.0.88 is reachable, NQA sends the result to the Track module. The Track module sets the track entry to Positive state.
   o When the next hop becomes unreachable, NQA sends the result to the Track module. The Track module sets the track entry to Negative state.
3. Associate the track entry with the static route.
   o When the track entry is in Positive state, the static routing module considers the static route to be valid.
   o When the track entry is in Negative state, the static routing module considers the static route to be invalid.

Track configuration task list

To implement the collaboration function, establish associations between the Track module and detection modules, and between the Track module and application modules.

To configure the Track module, perform the following tasks:

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Associating the Track module with a detection module</td>
</tr>
<tr>
<td>Associating Track with NQA</td>
</tr>
<tr>
<td>• Associating Track with BFD</td>
</tr>
<tr>
<td>• Associating Track with CFD</td>
</tr>
<tr>
<td>• Associating Track with interface management</td>
</tr>
<tr>
<td>• Associating Track with route management</td>
</tr>
<tr>
<td>• Associating Track with LLDP</td>
</tr>
</tbody>
</table>
Tasks at a glance

(Required.) Associating the Track module with an application module:
- Associating Track with VRRP
- Associating Track with static routing
- Associating Track with PBR
- Associating Track with Smart Link
- Associating Track with EVI IS-IS
- Associating Track with VPLS
- Associating Track with VXLAN
- Associating Track with MPLS L2VPN
- Associating Track with EAA
- Associating Track with ERPS

Associating the Track module with a detection module

Associating Track with NQA

NQA supports multiple operation types to analyze network performance and service quality. For example, an NQA operation can periodically detect whether a destination is reachable, or whether a TCP connection can be established.

An NQA operation operates as follows when it is associated with a track entry:
- If the consecutive failures reach the specified threshold, the NQA module notifies the Track module that the tracked object has malfunctioned. The Track module then sets the track entry to Negative state.
- If the specified threshold is not reached, the NQA module notifies the Track module that the tracked object is operating correctly. The Track module then sets the track entry to Positive state.

For more information about NQA, see Network Management and Monitoring Configuration Guide.

To associate Track with NQA:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>track track-entry-number nqa entry admin-name operation-tag reaction item-number [ delay { negative negative-time</td>
<td>positive positive-time } * ]</td>
</tr>
</tbody>
</table>

Associating Track with BFD

BFD supports the control packet mode and echo packet mode. A track entry can be associated only with the echo-mode BFD session. For more information about BFD, see "Configuring BFD."

The associated Track and BFD operate as follows:
- If the BFD detects that the link fails, it informs the Track module of the link failure. The Track module sets the track entry to Negative state.
• If the BFD detects that the link is operating correctly, the Track module sets the track entry to Positive state.

Before you associate Track with BFD, configure the source IP address of BFD echo packets. For more information, see "Configuring BFD."

To associate Track with BFD:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>track track-entry-number bfd echo interface interface-type interface-number remote ip remote-ip-address local ip local-ip-address [ delay { negative negative-time</td>
<td>positive positive-time } * ]</td>
</tr>
</tbody>
</table>

**Associating Track with CFD**

The associated Track and CFD operate as follows:

• If the CFD detects that the link fails, it informs the Track module of the link failure. The Track module then sets the track entry to Negative state.

• If the CFD detects that the link is operating correctly, the Track module sets the track entry to Positive state.

Before you associate Track with CFD, enable CFD and create a MEP. For more information, see "Configuring CFD."

To associate Track with CFD:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>track track-entry-number cfd cc service-instance instance-id mep mep-id [ delay { negative negative-time</td>
<td>positive positive-time } * ]</td>
</tr>
</tbody>
</table>

**Associating Track with interface management**

The interface management module monitors the link status or network-layer protocol status of interfaces. The associated Track and interface management operate as follows:

• When the link or network-layer protocol status of the interface changes to up, the interface management module informs the Track module of the change. The Track module sets the track entry to Positive state.

• When the link or network-layer protocol status of the interface changes to down, the interface management module informs the Track module of the change. The Track module sets the track entry to Negative state.

To associate Track with interface management:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
2. Create a track entry, and associate it with interface management.

- Create a track entry, and associate it with the interface management module to monitor the link status of an interface:
  \[
  \text{track track-entry-number interface interface-type interface-number [ delay \{ negative negative-time | positive positive-time \} * ]}
  \]

- Create a track entry, and associate it with the interface management module to monitor the physical status of an interface:
  \[
  \text{track track-entry-number interface interface-type interface-number physical [ delay \{ negative negative-time | positive positive-time \} * ]}
  \]

- Create a track entry, and associate it with the interface management module to monitor the network-layer protocol status of an interface:
  \[
  \text{track track-entry-number interface interface-type interface-number protocol \{ ipv4 | ipv6 \} [ delay \{ negative negative-time | positive positive-time \} * ]}
  \]

By default, no track entries exist.

### Associating Track with route management

The route management module monitors route entry changes in the routing table. The associated Track and route management operate as follows:

- When a monitored route entry is found in the routing table, the route management module informs the Track module. The Track module sets the track entry to Positive state.
- When a monitored route entry is removed from the routing table, the route management module informs the Track module of the change. The Track module sets the track entry to Negative state.

To associate Track with route management:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>track track-entry-number ip route [ vpn-instance vpn-instance-name ] ip-address { mask-length</td>
<td>mask } reachability [ delay { negative negative-time</td>
</tr>
</tbody>
</table>

### Associating Track with LLDP

The LLDP module monitors the neighbor availability of LLDP interfaces. The associated Track and LLDP operate as follows:

- When the neighbor of the monitored LLDP interface is available, the LLDP module informs the Track module. The Track module sets the track entry to Positive state.
When the neighbor of the monitored LLDP interface is unavailable, the LLDP module informs the Track module. The Track module sets the track entry to Negative state.

For more information about LLDP, see *Layer 2—LAN Switching Configuration Guide*.

To associate Track with LLDP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a track entry and associate it with an LLDP interface.</td>
<td>track track-entry-number lldp neighbor interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>delay { negative negative-time</td>
</tr>
</tbody>
</table>

### Associating the Track module with an application module

Before you associate the Track module with an application module, make sure the associated track entry has been created.

### Associating Track with VRRP

When VRRP is operating in standard 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 is not aware of the uplink failure. If the router is the master, hosts in the LAN cannot access the external network. To resolve this problem, configure a detection module-Track-VRRP collaboration. The detection module monitors the status of the uplink of the router and notifies the Track module of the detection result.
  - When the uplink fails, the detection module notifies the Track module to change the status of the monitored track entry to Negative. The priority of the master decreases by a user-specified value. A router with a higher priority in the VRRP group becomes the master.
- 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 VF to implement the following functions:

- Change the priority of the AVF according to its uplink state. When the uplink of the AVF fails, the track entry changes to Negative state. The weight of the AVF decreases by a user-specified value. The VF with a higher priority becomes the new AVF to forward packets.
- Monitor the AVF status from the LVF. When the AVF fails, the LVF that is operating in switchover mode becomes the new AVF to ensure continuous forwarding.

When you associate Track with VRRP, follow these restrictions and guidelines:

- VRRP tracking does not take effect on an IP address owner. The configuration takes effect when the router does not act as the IP address owner.
  - An IP address owner is the router with its interface IP address used as the virtual IP address of the VRRP group.
- When the status of the track entry changes from Negative to Positive or NotReady, the associated router or VF restores its priority automatically.
### Associating Track with a VRRP group

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Associate a track entry with a VRRP group.</td>
<td>By default, no track entry is specified for a VRRP group. This command is supported when VRRP is operating in both standard mode and load balancing mode.</td>
</tr>
</tbody>
</table>

### Associating Track with a VRRP VF

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Associate Track with a VRRP VF.</td>
<td>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 command takes effect only when VRRP is operating in load balancing mode.</td>
</tr>
</tbody>
</table>

### Associating Track with static routing

A static route is a manually configured route to route packets. For more information about static route configuration, see *Layer 3—IP Routing Configuration Guide*. Static routes cannot adapt to network topology changes. Link failures or network topological changes can make the routes unreachable and cause communication interruption.

To resolve 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.

To check the accessibility of a static route in real time, associate the Track module with the static route.

If you specify the next hop but not the output interface when configuring a static route, you can configure the static routing-Track-detection module collaboration. This collaboration enables you to verify the accessibility of the static route based on the track entry state.

- If the track entry is in Positive state, the following conditions exist:
  - The next hop of the static route is reachable.
  - The configured static route is valid.
- If the track entry is in Negative state, the following conditions exist:
  - The next hop of the static route is not reachable.
  - The configured static route is invalid.
- If the track entry is in NotReady state, the following conditions exist:
The accessibility of the next hop of the static route is unknown.

The static route is valid.

When you associate Track with static routing, follow these restrictions and guidelines:

- In static routing-Track-NQA collaboration, you must configure the same VPN instance name for the NQA operation and the next hop of the static route. Otherwise, the accessibility detection cannot operate correctly.
- If a static route needs route recursion, the associated track entry must monitor the next hop of the recursive route. The next hop of the static route cannot be monitored. Otherwise, a valid route might be considered invalid.

To associate Track with static routing:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Associate a static route with a track entry to check the accessibility of the next hop.</td>
<td></td>
</tr>
</tbody>
</table>

Method 1:

```
ip route-static { dest-address { mask-length | mask } | group group-name } { next-hop-address 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 ]
```

Method 2:

```
ip route-static vpn-instance s-vpn-instance-name { dest-address { mask-length | mask } | group group-name } { 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 ]
```

By default, Track is not associated with static routing.

Associating Track with PBR

PBR uses user-defined policies to route packets. You can specify parameters to guide the forwarding of the packets that match specific criteria. The parameters include the VPN instance, next hop, and default next hop. For more information about PBR, see Layer 3—IP Routing Configuration Guide.

PBR cannot detect the availability of any action taken on packets. When an action is not available, packets processed by the action might be discarded. For example, if the next hop specified for PBR fails, PBR cannot detect the failure, and continues to forward matching packets to the next hop.

To enable PBR to detect topology changes and improve the flexibility of the PBR application, configure Track-PBR-detection module collaboration.

After you associate a track entry with an apply clause, the detection module associated with the track entry sends Track the detection result of the availability of the tracked object.

- The Positive state of the track entry indicates that the object is available, and the apply clause is valid.
- The Negative state of the track entry indicates that the object is not available, and the apply clause is invalid.
- The NotReady state of the track entry indicates that the apply clause is valid.

The following objects can be associated with a track entry:

- Next hop.
- Default next hop.

**Configuration prerequisites**

Before you associate Track with PBR, create a policy or a policy node, and configure the match criteria.

**Configuration procedure**

To associate Track with PBR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>policy-based-route policy-name [ deny</td>
<td>permit ] node node-number</td>
</tr>
<tr>
<td>3.</td>
<td>• Define an ACL match criterion: if-match acl { acl-number</td>
<td>name acl-name }&lt;br&gt;• Define a local QoS ID match criterion: if-match qos-local-id local-id-value</td>
</tr>
<tr>
<td>4.</td>
<td>• Set the next hop, and associate it with a track entry: apply next-hop [ vpn-instance vpn-instance-name ] { ip-address [ direct ] [ track track-entry-number ] }&lt;1-n&gt;&lt;br&gt;• Set the default next hop, and associate it with a track entry: apply default-next-hop [ vpn-instance vpn-instance-name ] { ip-address [ direct ] [ track track-entry-number ] }&lt;1-n&gt;</td>
<td>Use a minimum of one command.</td>
</tr>
</tbody>
</table>

To associate Track with IPv6 PBR:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ipv6 policy-based-route policy-name [ deny</td>
<td>permit ] node node-number</td>
</tr>
<tr>
<td>3.</td>
<td>if-match acl { ipv6-acl-number</td>
<td>name ipv6-acl-name }</td>
</tr>
<tr>
<td>4.</td>
<td>apply next-hop [ vpn-instance vpn-instance-name ] { ipv6-address [ direct ] [ track track-entry-number ] }&lt;1-n&gt;</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Associating Track with Smart Link**

Smart Link cannot detect faults such as unidirectional links, misconnected fibers, or packet loss on intermediate devices or network paths of the uplink. It also cannot detect 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.

You can configure the collaboration between Smart Link and Track on a smart link group member port. Smart Link collaborates with the CC feature of CFD through the track entry to detect the link status on the port.
When the track entry is in Positive state, the link is in normal state. Smart Link does not perform link switchover for the smart link group.

When the track entry is in Negative state, the link has failed. Smart Link determines whether to perform link switchover according to the link preemption mode and port role configured in the smart link group.

When the track entry is in NotReady state, the port state does not change.

For more information about Smart Link, see “Configuring Smart Link.”

To configure collaboration between Smart Link and Track:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure collaboration between Smart Link and Track on the port.</td>
<td>port smart-link group group-id track track-entry-number</td>
</tr>
</tbody>
</table>

**Associating Track with EVI IS-IS**

EVI is a MAC-in-IP technology that provides Layer 2 connectivity between distant Layer 2 network sites across an IP routed network. It is used for connecting geographically dispersed sites of a virtualized large-scale data center that requires Layer 2 adjacency. EVI IS-IS establishes adjacencies and advertises MAC reachability information among edge devices at different sites in an EVI network.

EVI IS-IS uses a hello mechanism to monitor the connectivity of each EVI link on an EVI tunnel. To detect the connectivity of a particular EVI link more quickly, you can associate its tunnel interface with a track entry. The monitoring protocol used in this entry can only be BFD.

EVI IS-IS changes the state of an EVI-Link interface in response to the track entry state, as shown in Table 17.

**Table 17 EVI IS-IS action on the monitored EVI-Link in response to the track entry state change**

<table>
<thead>
<tr>
<th>Track entry state</th>
<th>State of the monitored EVI link</th>
<th>EVI IS-IS action on the EVI-Link interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive</td>
<td>The EVI link is operating correctly.</td>
<td>Places the EVI-Link interface in up state.</td>
</tr>
<tr>
<td>Negative</td>
<td>The EVI link has failed.</td>
<td>Places the EVI-Link interface in down state.</td>
</tr>
<tr>
<td>NotReady</td>
<td>The EVI link is not monitored.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
For more information about EVI IS-IS, see *EVI Configuration Guide*.

To associate an EVI tunnel interface with a track entry:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter EVI tunnel interface view.</td>
<td>interface tunnel number [ mode evi [ ipv6 ] ] N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Associate a track entry with the tunnel interface.</td>
<td>evi isis track track-entry-number By default, an EVI tunnel interface is not associated with any track entries. You can associate an EVI tunnel interface with only one track entry.</td>
</tr>
</tbody>
</table>

**Associating Track with VPLS**

When you associate Track with an AC (an Ethernet service instance) on a VPLS network, the AC is up only when one or more of the associated track entries are positive.

To associate an Ethernet service instance with a track entry:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>• Enter Layer 2 Ethernet interface view: interface interface-type interface-number • Enter Layer 2 aggregate interface view: interface bridge-aggregation interface-number N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Create an Ethernet service instance and enter Ethernet service instance view.</td>
<td>service-instance instance-id By default, no Ethernet service instances exist.</td>
</tr>
<tr>
<td>4.</td>
<td>Bind the Ethernet service instance to a VSI and associate it with a track entry.</td>
<td>xconnect vsi vsi-name [ access-mode { ethernet</td>
</tr>
</tbody>
</table>

**Associating Track with VXLAN**

To monitor the status of an AC (an Ethernet service instance) on a VXLAN network, associate it with track entries. The AC is up only when one or more of the associated track entries are positive.

To associate an Ethernet service instance with a track entry:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **2.** Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view. | • Enter Layer 2 Ethernet interface view: <interface> interface-type <interface-number>  
• Enter Layer 2 aggregate interface view: <interface> bridge-aggregation <interface-number> | N/A |
| **3.** Create an Ethernet service instance and enter its view. | **service-instance instance-id** | By default, no Ethernet service instances exist. |
| **4.** Bind the Ethernet service instance to a VSI and associate it with a track entry. | **xconnect vsi vsi-name**  
[ access-mode { ethernet | vlan } ]  
**track track-entry-number**&<1-3> | By default, an Ethernet service instance is not bound to any VSI or associated with any track entry. |

## Associating Track with MPLS L2VPN

When you bind an AC (an Ethernet service instance) to a cross-connect on an MPLS L2VPN network, you can associate Track with the AC. Then, the AC is up only when one or more of the associated track entries are positive.

To associate a track entry with an Ethernet service instance bound to a non-BGP cross-connect:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong> Enter system view.</td>
<td><strong>system-view</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>2.</strong> Enter cross-connect group view.</td>
<td><strong>xconnect-group group-name</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>3.</strong> Enter cross-connect view.</td>
<td><strong>connection connection-name</strong></td>
<td>N/A</td>
</tr>
</tbody>
</table>
| **4.** Bind the Ethernet service instance on the interface to the non-BGP cross-connect and associate the service instance with a track entry. | **ac interface** interface-type <interface-number>  
**service-instance instance-id**  
[ access-mode { ethernet | vlan } ]  
**track track-entry-number**&<1-3> | By default, the Ethernet service instance is not bound to any cross-connect or associated with any track entry. |

To associate a track entry with an Ethernet service instance bound to a BGP cross-connect:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong> Enter system view.</td>
<td><strong>system-view</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>2.</strong> Enter cross-connect group view.</td>
<td><strong>xconnect-group group-name</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>3.</strong> Enter auto-discovery cross-connect group view.</td>
<td><strong>auto-discovery bgp</strong></td>
<td>N/A</td>
</tr>
</tbody>
</table>
| **4.** Enter site view. | **site site-id**  
[ range range-value ]  
[ default-offset default-offset-value ] | N/A |
| **5.** Enter auto-discovery cross-connect view. | **connection remote-site-id**  
**remote-site-id** | N/A |
6. Bind the Ethernet service instance on the interface to the BGP cross-connect and associate the service instance with a track entry.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a CLI-defined monitor policy and enter its view, or enter the view of an existing CLI-defined monitor policy.</td>
<td>rtm cli-policy policy-name</td>
</tr>
<tr>
<td>3.</td>
<td>Configure a track event.</td>
<td>event track track-entry-number-list state { negative</td>
</tr>
</tbody>
</table>

**Associating Track with EAA**

Embedded Automation Architecture (EAA) is a monitoring framework that enables you to self-define monitored events and the actions to take. It allows you to create monitor policies by using the CLI or Tcl scripts.

For more information about EAA, see *Network Management and Monitoring Configuration Guide*.

You can configure EAA track event monitor policies to monitor the positive-to-negative or negative-to-positive state changes of track entries.

- If you specify only one track entry for a policy, EAA triggers the policy when it detects the specified state change on the track entry.
- If you specify multiple track entries for a policy, EAA triggers the policy when it detects the specified state change on the last monitored track entry. For example, if you configure a policy to monitor the positive-to-negative state change of multiple track entries, EAA triggers the policy when the last positive track entry monitored by the policy changes to the Negative state.

You can set a suppression time for a track event monitor policy. The timer starts when the policy is triggered. The system does not process messages that report the monitored track event until the timer times out.

To configure a track event monitor policy:

**Associating Track with ERPS**

To detect and clear link faults typically for a fiber link, use ERPS with CFD and Track. You can associate ERPS ring member ports with the continuity check function of CFD through track entries. CFD reports link events only when the monitored VLAN is the control VLAN of the ERPS instance for the port.

Track changes the track entry state based on the monitoring result of CFD, and notifies the track entry state change to the associated EPRS ring.

- When the track entry is in Positive state, the link of the monitored ERPS ring member port is in normal state. The ERPS ring does not switch traffic to other links.
- When the track entry is in Negative state, the link of the monitored ERPS ring member port is faulty. The ERPS ring switches traffic to other links.
• When the track entry is in NotReady state, the state of the ERPS ring member port does not change.

Before you associate a port with a track entry, make sure the port has joined an ERPS instance.

For more information about ERPS, see "Configuring ERPS."

To associate an ERPS ring member port with a track entry:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Associate an ERPS ring member port with a track entry.</td>
<td>port erps ring ring-id instance instance-id track track-entry-index</td>
</tr>
</tbody>
</table>

Displaying and maintaining track entries

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about track entries.</td>
<td>`display track { track-entry-number</td>
</tr>
</tbody>
</table>

Track configuration examples

VRRP-Track-NQA collaboration configuration example

Network requirements

As shown in Figure 59:

• Host A requires access to Host B. The default gateway of Host A is 10.1.1.10/24.
• Switch A and Switch B belong to VRRP group 1. The virtual IP address of VRRP group 1 is 10.1.1.10.

Configure VRRP-Track-NQA collaboration to monitor the uplink on the master and meet the following requirements:

• When Switch A operates correctly, Switch A forwards packets from Host A to Host B.
• When NQA detects a fault on the uplink of Switch A, Switch B forwards packets from Host A to Host B.
Configuration procedure

1. Create VLANs and assign ports to them. Configure the IP address of each VLAN interface, as shown in Figure 59. (Details not shown.)

2. Configure an NQA operation on Switch A:
   
   # Create an NQA operation with administrator name admin and operation tag test.
   
   `<SwitchA> system-view
   [SwitchA] nqa entry admin test
   # Configure the operation type as ICMP echo.
   [SwitchA-nqa-admin-test] type icmp-echo
   # Specify 10.1.2.2 as the destination address of ICMP echo requests.
   [SwitchA-nqa-admin-test-icmp-echo] destination ip 10.1.2.2
   # Configure the ICMP echo operation to repeat every 100 milliseconds.
   [SwitchA-nqa-admin-test-icmp-echo] frequency 100
   # Configure reaction entry 1, specifying that five consecutive probe failures trigger the Track module.
   [SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
   [SwitchA-nqa-admin-test-icmp-echo] quit
   # Start the NQA operation.
   [SwitchA] nqa schedule admin test start-time now lifetime forever

3. On Switch A, configure track entry 1, and associate it with reaction entry 1 of the NQA operation.
   
   [SwitchA] track 1 nqa entry admin test reaction 1

4. Configure VRRP on Switch A:
   
   # Specify VRRPV2 to run on the interface VLAN-interface 2.
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] vrrp version 2
   # Create VRRP group 1, and configure the virtual IP address 10.1.1.10 for the group.
   [SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
   # Set the priority of Switch A to 110 in VRRP group 1.
   [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 every 500 centiseconds.
[SwitchA-Vlan-interface2] vrrp vrid 1 timer advertise 500

# Configure Switch A to operate in preemptive mode and set the preemption delay to 5000 centiseconds.
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5000

# Associate VRRP group 1 with track entry 1 and decrease the router priority by 30 when the state of track entry 1 changes to negative.
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 30

5. Configure VRRP on Switch B:

# Specify VRRPv2 to run on the interface VLAN-interface 2.
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp version 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 every 500 centiseconds.
[SwitchB-Vlan-interface2] vrrp vrid 1 timer advertise 500

# Configure Switch B to operate in preemptive mode and set the preemption delay to 5000 centiseconds.
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5000

Verifying the configuration

# Ping Host B from Host A to verify that Host B is reachable. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.
[SwitchA-Vlan-interface2] display vrrp verbose
IPV4 Virtual Router Information:
Running Mode : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
    VRID : 1           Adver Timer : 500
    Admin Status : Up    State : Master
    Config Pri  : 110    Running Pri : 110
    Preempt Mode : Yes    Delay Time : 5000
    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 Virtual Router Information:
Running Mode : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
The output shows that in VRRP group 1, Switch A is the master, and Switch B is a backup. Switch A forwards packets from Host A to Host B.

`# Disconnect the link between Switch A and Switch C, and verify that Host A can still ping Host B. (Details not shown.)`

`# Display detailed information about VRRP group 1 on Switch A.
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode : Standard
  Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID : 1   Adver Timer : 500
    Admin Status : Up   State : Backup
    Config Pri : 110   Running Pri : 80
    Preempt Mode : Yes   Delay Time : 5000
    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.
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode : Standard
  Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID : 1   Adver Timer : 500
    Admin Status : Up   State : Master
    Config Pri : 100   Running Pri : 100
    Preempt Mode : Yes   Delay Time : 5000
    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 Switch A becomes the backup, and Switch B becomes the master. Switch B forwards packets from Host A to Host B.
Configuring BFD for a VRRP backup to monitor the master

Network requirements

As shown in Figure 60:

- Switch A and Switch B belong to VRRP group 1. The virtual IP address of VRRP group 1 is 192.168.0.10.
- The default gateway of the hosts in the LAN is 192.168.0.10.

Configure VRRP-Track-BFD collaboration to monitor the master on the backup and meet the following requirements:

- When Switch A operates correctly, the hosts in the LAN access the Internet through Switch A.
- When Switch A fails, the backup (Switch B) can detect the state change of the master through BFD and become the new master. The hosts in the LAN access the Internet through Switch B.

Figure 60 Network diagram

Configuration procedure

1. Create VLANs and assign ports to them. Configure the IP address of each VLAN interface, as shown in Figure 60. (Details not shown.)
2. Configure Switch A:
   
   # Create VRRP group 1, and configure the virtual IP address 192.168.0.10 for the group.
   <SwitchA> system-view
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
   # Set the priority of Switch A to 110 in VRRP group 1.
   [SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
   [SwitchA-Vlan-interface2] return
3. Configure Switch B:

# Specify 10.10.10.10 as the source address of BFD echo packets.
<SwitchB> system-view
[SwitchB] bfd echo-source-ip 10.10.10.10

# Create track entry 1, and associate it with the BFD session to verify the reachability of Switch A.
[SwitchB] track 1 bfd echo interface vlan-interface 2 remote ip 192.168.0.101 local ip 192.168.0.102

# Create VRRP group 1, and configure the virtual IP address 192.168.0.10 for the group.
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10

# Configure VRRP group 1 to monitor the status of track entry 1.
[SwitchB-Vlan-interface2] vrrp vrid 1 track 1 switchover
[SwitchB-Vlan-interface2] return

Verifying the configuration

# Display detailed information about VRRP group 1 on Switch A.
<SwitchA> display vrrp verbose
IPv4 Virtual Router Information:
Running Mode : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID : 1              Adver Timer : 100
  Admin Status : Up      State : Master
  Config Pri : 110         Running Pri : 110
  Preempt Mode : Yes     Delay Time : 0
  Auth Type : None
  Virtual IP : 192.168.0.10
  Virtual MAC : 0000-5e00-0101
  Master IP : 192.168.0.101

# Display detailed information about VRRP group 1 on Switch B.
<SwitchB> display vrrp verbose
IPv4 Virtual Router Information:
Running Mode : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID : 1              Adver Timer : 100
  Admin Status : Up      State : Backup
  Config Pri : 100         Running Pri : 100
  Preempt Mode : Yes     Delay Time : 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
State: Positive
Duration: 0 days 0 hours 0 minutes 32 seconds
Notification delay: Positive 0, Negative 0 (in seconds)
Tracked object:
  BFD session mode: Echo
Outgoing interface: Vlan-interface2
VPN instance name: -
  Remote IP: 192.168.0.101
  Local IP: 192.168.0.102

The output shows that when the status of the track entry becomes Positive, Switch A is the master and Switch B is the backup.

# Enable VRRP state debugging and BFD event notification debugging on Switch B.
<SwitchB> terminal debugging
<SwitchB> terminal monitor
<SwitchB> debugging vrrp fsm
<SwitchB> debugging bfd ntfy

# When Switch A fails, the following output is displayed on Switch B.
*Dec 17 14:44:34:142 2008 SwitchB BFD/7/DEBUG: Notify application:TRACK State:DOWN
*Dec 17 14:44:34:144 2008 SwitchB VRRP4/7/FSM:
  IPv4 Vlan-interface2 | Virtual Router 1 : Backup --> Master  reason: The status of the tracked object changed

# Display detailed information about the VRRP group on Switch B.
<SwitchB> display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode      : Standard
  Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID           : 1               Adver Timer  : 100
    Admin Status   : Up              State        : Master
    Config Pri     : 100             Running Pri  : 100
    Preempt Mode   : Yes             Delay Time   : 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, the Track module notifies VRRP to change the status of Switch B to master. The backup can quickly preempt as the master without waiting for a period three times the advertisement interval plus the Skew_Time.

Configuring BFD for the VRRP master to monitor the uplinks

Network requirements

As shown in Figure 61:
  • Switch A and Switch B belong to VRRP group 1. The virtual IP address of VRRP group 1 is 192.168.0.10.
The default gateway of the hosts in the LAN is 192.168.0.10.

Configure VRRP-Track-BFD collaboration to monitor the uplink on the master and meet the following requirements:

- When Switch A operates correctly, the hosts in the LAN access the Internet through Switch A.
- When Switch A detects that the uplink is down through BFD, Switch B can preempt as the master. The hosts in the LAN can access the Internet through Switch B.

**Figure 61 Network diagram**

**Configuration procedure**

1. Create VLANs and assign ports to them. Configure the IP address of each VLAN interface, as shown in Figure 61. (Details not shown.)

2. Configure Switch A:
   
   ```
   # Specify 10.10.10.10 as the source address of BFD echo packets.
   <SwitchA> system-view
   [SwitchA] bfd echo-source-ip 10.10.10.10
   # Create track entry 1 for the BFD session to verify the reachability of the uplink device (1.1.1.2).
   [SwitchA] track 1 bfd echo interface vlan-interface 3 remote ip 1.1.1.2 local ip 1.1.1.1
   # Create VRRP group 1, and specify 192.168.0.10 as the virtual IP address of the group.
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
   # Set the priority of Switch A to 110 in VRRP group 1.
   [SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
   # Associate VRRP group 1 with track entry 1 and decrease the router priority by 20 when the state of track entry 1 changes to negative.
   [SwitchA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 20
   ```
3. On Switch B, create VRRP group 1, and specify 192.168.0.10 as the virtual IP address of the group.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
[SwitchB-Vlan-interface2] return
```

**Verifying the configuration**

```
# Display detailed information about the VRRP group on Switch A.
<SwitchA> display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode : Standard
  Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID           : 1               Adver Timer  : 100
    Admin Status   : Up              State        : Master
    Config Pri     : 110             Running Pri : 110
    Preempt Mode   : Yes             Delay Time   : 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 information about track entry 1 on Switch A.
<SwitchA> display track 1
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
```

```
# Display detailed information about the VRRP group on Switch B.
<SwitchB> display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode : Standard
  Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID           : 1               Adver Timer  : 100
    Admin Status   : Up              State        : Backup
    Config Pri     : 100             Running Pri : 100
    Preempt Mode   : Yes             Delay Time   : 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 is the backup.

# Display information about track entry 1 when the uplink of Switch A goes down.
<SwitchA> display track 1
Track ID: 1
State: Negative
Duration: 0 days 0 hours 0 minutes 32 seconds
Notification delay: Positive 0, Negative 0 (in seconds)
Tracked object:
  BFD session mode: Echo
  Outgoing interface: Vlan-interface2
VPN instance name: -
  Remote IP: 1.1.1.2
  Local IP: 1.1.1.1

# Display detailed information about VRRP group 1 on Switch A.
<SwitchA> display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode : Standard
  Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID : 1       Adver Timer : 100
    Admin Status : Up       State : Backup
    Config Pri : 110       Running Pri : 90
    Preempt Mode : Yes       Delay Time : 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 detailed information about VRRP group 1 on Switch B.
<SwitchB> display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode : Standard
  Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID : 1       Adver Timer : 100
    Admin Status : Up       State : Master
    Config Pri : 100       Running Pri : 100
    Preempt Mode : Yes       Delay Time : 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. Switch B then preempts as the master.

Static routing-Track-NQA collaboration configuration example

Network requirements

As shown in Figure 62:

- Switch A is the default gateway of the hosts in network 20.1.1.0/24.
- Switch D is the default gateway of the hosts in network 30.1.1.0/24.
- Hosts in the two networks communicate with each other through static routes.

To ensure network availability, configure route backup and static routing-Track-NQA collaboration on Switch A and Switch D as follows:

- On Switch A, assign a higher priority to the static route to 30.1.1.0/24 with the next hop Switch B. This route is the master route. The static route to 30.1.1.0/24 with the next hop Switch C acts as the backup route. When the master route is unavailable, the backup route takes effect. Switch A forwards packets to 30.1.1.0/24 through Switch C.
- On Switch D, assign a higher priority to the static route to 20.1.1.0/24 with the next hop Switch B. This route is the master route. The static route to 20.1.1.0/24 with the next hop Switch C acts as the backup route. When the master route is unavailable, the backup route takes effect. Switch D forwards packets to 20.1.1.0/24 through Switch C.

Figure 62 Network diagram

Configuration procedure

1. Create VLANs and assign ports to them. Configure the IP address of each VLAN interface, as shown in Figure 62. (Details not shown.)

2. Configure Switch A:

   # Configure a static route to 30.1.1.0/24 with the next hop 10.1.1.2 and the default priority 60. Associate this static route 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 next hop 10.3.1.3 and the priority 80.
### Configure Switch A:

- **Static Route Configuration**:
  - `ip route-static 30.1.1.0 24 10.3.1.3 preference 80`  
  # Configure a static route to 30.1.1.0/24 with the next hop 10.3.1.3.

- **NQA Configuration**:
  - `nqa entry admin test`  
  # Create an NQA operation with administrator admin and operation tag test.

- **Operation Configuration**:
  - `ip route-static 10.2.1.4 24 10.1.1.2`  
  # Configure a static route to 10.2.1.4 with the next hop 10.1.1.2.
  
  - `nqa entry admin test`  
  # Configure the operation type as ICMP echo.

- **Response Configuration**:
  - `frequency 100`  
  # Configure the ICMP echo operation to repeat every 100 milliseconds.

- **Reaction Configuration**:
  - `reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only`  
  # Configure reaction entry 1, specifying that five consecutive probe failures trigger the Track module.

- **Schedule Configuration**:
  - `nqa schedule admin test start-time now lifetime forever`  
  # Start the NQA operation.

### Configure Switch B:

- **Static Route Configuration**:
  - `ip route-static 30.1.1.0 24 10.2.1.4`  
  # Configure a static route to 30.1.1.0/24 with the next hop 10.2.1.4.

- **Static Route Configuration**:
  - `ip route-static 20.1.1.0 24 10.1.1.1`  
  # Configure a static route to 20.1.1.0/24 with the next hop 10.1.1.1.

### Configure Switch C:

- **Static Route Configuration**:
  - `ip route-static 30.1.1.0 24 10.4.1.4`  
  # Configure a static route to 30.1.1.0/24 with the next hop 10.4.1.4.

- **Static Route Configuration**:
  - `ip route-static 20.1.1.0 24 10.3.1.1`  
  # Configure a static route to 20.1.1.0/24 with the next hop 10.3.1.1.

### Configure Switch D:

- **Static Route Configuration**:
  - `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 next hop 10.2.1.2 and the default priority 60. Associate this static route with track entry 1.

- **Static Route Configuration**:
  - `ip route-static 20.1.1.0 24 10.4.1.3 preference 80`  
  # Configure a static route to 20.1.1.0/24 with the next hop 10.4.1.3 and the priority 80.

- **Static Route Configuration**:
  - `ip route-static 10.1.1.1 24 10.2.1.2`  
  # Configure a static route to 10.1.1.1 with the next hop 10.2.1.2.

- **NQA Configuration**:
  - `nqa entry admin test`  
  # Create an NQA operation with administrator admin and operation tag test.

- **Operation Configuration**:
  - `ip route-static 10.2.1.4 24 10.1.1.2`  
  # Configure a static route to 10.2.1.4 with the next hop 10.1.1.2.

- **Operation Configuration**:
  - `nqa entry admin test`  
  # Configure the operation type as ICMP echo.

### Additional Configuration Options:

- `system-view`  
  # Switch commands.

- `quit`  
  # Exit configuration mode.

- `type icmp-echo`  
  # Specify the ICMP echo operation type.
# Specify 10.1.1.1 as the destination address of the operation.
[SwitchD-nqa-admin-test-icmp-echo] destination ip 10.1.1.1

# Specify 10.2.1.2 as the next hop of the operation.
[SwitchD-nqa-admin-test-icmp-echo] next-hop ip 10.2.1.2

# Configure the ICMP echo operation to repeat every 100 milliseconds.
[SwitchD-nqa-admin-test-icmp-echo] frequency 100

# Configure reaction entry 1, specifying that five consecutive probe failures trigger the Track module.
[SwitchD-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail
threshold-type consecutive 5 action-type trigger-only
[SwitchD-nqa-admin-test-icmp-echo] quit

# Start the NQA operation.
[SwitchD] nqa schedule admin test start-time now lifetime forever

# Configure track entry 1, and associate it with reaction entry 1 of the NQA operation.
[SwitchD] track 1 nqa entry admin test reaction 1

Verifying the configuration

# Display information about the track entry on Switch A.
[SwitchA] display track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 1
    Remote IP/URL: --
    Local IP: --
    Interface: --

The output shows that the status of the track entry is Positive, indicating that the NQA operation has succeeded and the master route is available.

# Display the routing table of Switch A.
[SwitchA] display ip routing-table

<table>
<thead>
<tr>
<th>Destination/Prefix</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>10.1.1.1</td>
<td>Vlan2</td>
</tr>
<tr>
<td>10.1.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>10.2.1.0/24</td>
<td>Static</td>
<td>60</td>
<td>0</td>
<td>10.1.1.2</td>
<td>Vlan2</td>
</tr>
<tr>
<td>10.3.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>10.3.1.1</td>
<td>Vlan3</td>
</tr>
<tr>
<td>10.3.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>20.1.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>20.1.1.1</td>
<td>Vlan6</td>
</tr>
<tr>
<td>20.1.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>30.1.1.0/24</td>
<td>Static</td>
<td>60</td>
<td>0</td>
<td>10.1.1.2</td>
<td>Vlan2</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
</tbody>
</table>

The output shows that 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
State: Negative
Duration: 0 days 0 hours 0 minutes 32 seconds
Notification delay: Positive 0, Negative 0 (in seconds)
Tracked object:
  NQA entry: admin test
  Reaction: 1
  Remote IP/URL: --
  Local IP: --
  Interface: --

The output shows that the status of the track entry is Negative, indicating that the NQA operation has failed and the master route is unavailable.

# Display the routing table of Switch A.

[SwitchA] display ip routing-table

Destinations : 10 Routes : 10

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>10.1.1.1</td>
<td>Vlan2</td>
</tr>
<tr>
<td>10.1.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>10.2.1.0/24</td>
<td>Static</td>
<td>60</td>
<td>0</td>
<td>10.1.1.2</td>
<td>Vlan2</td>
</tr>
<tr>
<td>10.3.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>10.3.1.1</td>
<td>Vlan3</td>
</tr>
<tr>
<td>10.3.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>20.1.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>20.1.1.1</td>
<td>Vlan6</td>
</tr>
<tr>
<td>20.1.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>30.1.1.0/24</td>
<td>Static</td>
<td>80</td>
<td>0</td>
<td>10.3.1.3</td>
<td>Vlan3</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.0.0.0.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
</tbody>
</table>

The output shows that Switch A forwards packets to 30.1.1.0/24 through Switch C. The backup static route has taken effect.

# Verify that hosts in 20.1.1.0/24 can communicate with the hosts in 30.1.1.0/24 when the master route fails.

[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

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
Static routing-Track-BFD collaboration configuration example

Network requirements

As shown in Figure 63:

- Switch A is the default gateway of the hosts in network 20.1.1.0/24.
- Switch B is the default gateway of the hosts in network 30.1.1.0/24.
- Hosts in the two networks communicate with each other through static routes.

To ensure network availability, configure route backup and static routing-Track-BFD collaboration on Switch A and Switch B as follows:

- On Switch A, assign a higher priority to the static route to 30.1.1.0/24 with the next hop Switch B. This route is the master route. The static route to 30.1.1.0/24 with the next hop Switch C acts as the backup route. When the master route is unavailable, BFD can quickly detect the route failure to make the backup route take effect.

- On Switch B, assign a higher priority to the static route to 20.1.1.0/24 with the next hop Switch A. This route is the master route. The static route to 20.1.1.0/24 with the next hop Switch C acts as the backup route. When the master route is unavailable, BFD can quickly detect the route failure to make the backup route take effect.

Figure 63 Network diagram

Configuration procedure

1. Create VLANs and assign ports to them. Configure the IP address of each VLAN interface, as shown in Figure 63. (Details not shown.)
2. Configure Switch A:

# Configure a static route to 30.1.1.0/24 with the next hop 10.2.1.2 and the default priority 60.
Associate this static route 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 next hop 10.3.1.3 and the priority 80.

[SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80

# Specify 10.10.10.10 as the source address of BFD echo packets.

[SwitchA] bfd echo-source-ip 10.10.10.10

# Configure track entry 1, and associate it with the BFD session to verify the connectivity between Switch A and 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 next hop 10.2.1.1 and the default priority 60.
Associate this static route 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 next hop 10.4.1.3 and the priority 80.

[SwitchB] ip route-static 20.1.1.0 24 10.4.1.3 preference 80

# Specify 1.1.1.1 as the source address of BFD echo packets.

[SwitchB] bfd echo-source-ip 1.1.1.1

# Configure track entry 1, and associate it with the BFD session to verify the connectivity between Switch B and Switch A.

[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 next hop 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 next hop 10.3.1.1.

[SwitchB] ip route-static 20.1.1.0 24 10.3.1.1

Verifying the configuration

# Display information about the track entry on Switch A.

[SwitchA] display track all

Track ID: 1
State: Positive
Duration: 0 days 0 hours 0 minutes 32 seconds
Notification delay: Positive 0, Negative 0 (in seconds)
Tracked object:
  BFD session mode: Echo
  Outgoing interface: Vlan-interface2
VPN instance name: -
  Remote IP: 10.2.1.2
  Local IP: 10.2.1.1

The output shows that the status of the track entry is Positive, indicating that the next hop 10.2.1.2 is reachable.
# Display the routing table of Switch A.

[SwitchA] display ip routing-table

Destinations : 9 Routes : 9

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>10.2.1.1</td>
<td>Vlan2</td>
</tr>
<tr>
<td>10.2.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>10.3.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>10.3.1.1</td>
<td>Vlan3</td>
</tr>
<tr>
<td>10.3.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>20.1.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>20.1.1.1</td>
<td>Vlan5</td>
</tr>
<tr>
<td>20.1.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>30.1.1.0/24</td>
<td>Static</td>
<td>60</td>
<td>0</td>
<td>10.3.1.3</td>
<td>Vlan3</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
</tbody>
</table>

The output shows that Switch A forwards packets to 30.1.1.0/24 through Switch B. The master static route has taken effect.

# Remove the IP address of 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
State: Negative
Duration: 0 days 0 hours 0 minutes 32 seconds
Notification delay: Positive 0, Negative 0 (in seconds)
Tracked object:
  BFD session mode: Echo
  Outgoing interface: Vlan-interface2
  VPN instance name: -
  Remote IP: 10.2.1.2
  Local IP: 10.2.1.1

The output shows that the status of the track entry is Negative, indicating that the next hop 10.2.1.2 is unreachable.

# Display the routing table of Switch A.

[SwitchA] display ip routing-table

Destinations : 9 Routes : 9

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>10.2.1.1</td>
<td>Vlan2</td>
</tr>
<tr>
<td>10.2.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>10.3.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>10.3.1.1</td>
<td>Vlan3</td>
</tr>
<tr>
<td>10.3.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>20.1.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>20.1.1.1</td>
<td>Vlan5</td>
</tr>
<tr>
<td>20.1.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>30.1.1.0/24</td>
<td>Static</td>
<td>80</td>
<td>0</td>
<td>10.3.1.3</td>
<td>Vlan3</td>
</tr>
</tbody>
</table>
The output shows that Switch A forwards packets to 30.1.1.0/24 through Switch C. The backup static route has taken effect.

# Verify that the hosts in 20.1.1.0/24 can communicate with the hosts in 30.1.1.0/24 when the master route fails.

```bash
[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

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

# Verify that the hosts in 30.1.1.0/24 can still communicate with the hosts in 20.1.1.0/24 when the master route fails.

```bash
[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

--- Ping statistics for 20.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

### VRRP-Track-interface management collaboration configuration example

#### Network requirements

As shown in Figure 64:

- Host A requires access to Host B. The default gateway of Host A is 10.1.1.10/24.
- Switch A and Switch B belong to VRRP group 1. The virtual IP address of VRRP group 1 is 10.1.1.10.

Configure VRRP-Track-interface management collaboration to monitor the uplink interface on the master and meet the following requirements:

- When Switch A operates correctly, Switch A forwards packets from Host A to Host B.
- When VRRP detects a fault on the uplink interface of Switch A through the interface management module, Switch B forwards packets from Host A to Host B.
**Configuration procedure**

1. Create VLANs and assign ports to them. Configure the IP address of each VLAN interface, as shown in Figure 64. (Details not shown.)

2. Configure Switch A:
   - # Configure track entry 1 and associate it with the link status of the uplink interface VLAN-interface 3.
     ```
     [SwitchA] track 1 interface vlan-interface 3
     ```
   - # 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 to 110 in VRRP group 1.
     ```
     [SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
     ```
   - # Associate VRRP group 1 with track entry 1 and decrease the router priority by 30 when the state of track entry 1 changes to negative.
     ```
     [SwitchA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 30
     ```

3. On Switch B, create VRRP group 1, and configure the virtual IP address 10.1.1.10 for the group.
   ```
   <SwitchB> system-view
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
   ```

**Verifying the configuration**

# Ping Host B from Host A to verify that Host B is reachable. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode : Standard
  Total number of virtual routers : 1
  Interface Vlan-interface2
  VRID : 1   Adver Timer : 100
  Admin Status : Up   State : Master
  Config Pri : 110   Running Pri : 110
  Preempt Mode : Yes   Delay Time : 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 Virtual Router Information:
Running Mode : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID : 1  Adver Timer : 100
  Admin Status : Up  State : Backup
  Config Pri : 100  Running Pri : 100
  Preempt Mode : Yes  Delay Time : 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. Switch A forwards packets from Host A to Host B.

# Shut down the uplink interface VLAN-interface 3 on Switch A.
[SwitchA-Vlan-interface2] interface vlan-interface 3
[SwitchA-Vlan-interface3] shutdown

# Ping Host B from Host A to verify that Host B is reachable. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.
[SwitchA-Vlan-interface3] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
  VRID : 1  Adver Timer : 100
  Admin Status : Up  State : Backup
  Config Pri : 110  Running Pri : 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

# Display detailed information about VRRP group 1 on Switch B.
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode : Standard
Total number of virtual routers : 1
VRRP-Track-route management collaboration configuration example

Network requirements

As shown in Figure 65:

- Host A requires access to Host B. The default gateway of Host A is 10.1.1.10/24.
- Switch A and Switch B belong to VRRP group 1. The virtual IP address of VRRP group 1 is 10.1.1.10.
- BGP peer relationships are established between Switch A and Switch C and between Switch B and Switch D. Switch C and Switch D advertise the default route 0.0.0.0/0 to Switch A and Switch B.

Configure VRRP-Track-route management collaboration to meet the following requirements:

- When Switch A operates correctly, Switch A forwards packets from Host A to Host B.
- When VRRP detects the removal of the default route from the routing table of Switch A through route management, Switch B forwards packets from Host A to Host B.

Figure 65 Network diagram

Configuration procedure

1. Configure the IP address of each interface, as shown in Figure 65. (Details not shown.)
2. Establish an IBGP peer relationship between Switch A and Switch C, and configure Switch C to advertise the default route 0.0.0.0/0 to Switch A.
<SwitchA> system-view
[SwitchA] bgp 100
[SwitchA-bgp-default] peer 10.1.2.2 as-number 100
[SwitchA-bgp-default] address-family ipv4
[SwitchA-bgp-default-ipv4] peer 10.1.2.2 enable

<SwitchC> system-view
[SwitchC] bgp 100
[SwitchC-bgp-default] peer 10.1.2.1 as-number 100
[SwitchC-bgp-default] address-family ipv4
[SwitchC-bgp-default-ipv4] peer 10.1.2.1 enable
[SwitchC-bgp-default-ipv4] peer 10.1.2.1 default-route-advertise
[SwitchC-bgp-default-ipv4] quit

3. Configure Switch B and Switch D in the same way Switch A and Switch C are configured. (Details not shown.)

4. Configure Track and VRRP on Switch A:
   # Configure track entry 1, and associate it with the default route 0.0.0.0/0.
   [SwitchA] track 1 ip route 0.0.0.0 0.0.0.0 reachability
   # 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 to 110 in VRRP group 1.
   [SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
   # Associate VRRP group 1 with track entry 1 and decrease the Switch priority by 30 when the state of track entry 1 changes to negative.
   [SwitchA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 30
   [SwitchA-Vlan-interface2] quit

5. On Switch B, create VRRP group 1, and configure the virtual IP address 10.1.1.10 for the group.
   <SwitchB> system-view
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
   [SwitchB-Vlan-interface2] quit

Verifying the configuration
   # Ping Host B from Host A to verify that Host B is reachable. (Details not shown.)
   # Display detailed information about VRRP group 1 on Switch A.
   [SwitchA] display vrrp verbose
   IPv4 Virtual Router Information:
   Running Mode : Standard
   Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID : 1     Adver Timer : 100
     Admin Status : Up     State : Master
     Config Pri : 110     Running Pri : 110
     Preempt Mode : Yes     Delay Time : 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] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode       : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
    VRID : 1         Adver Timer : 100
    Admin Status : Up         State : Backup
    Config Pri : 100         Running Pri : 100
    Preempt Mode : Yes         Delay Time : 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. Switch A forwards packets from Host A to Host B.

# Disable Switch C from exchanging routing information with Switch A so that the default route 0.0.0.0/0 is removed from the routing table of Switch A.
[SwitchC-bgp-default-ipv4] undo peer 10.1.2.1 enable

# Ping Host B from Host A to verify that Host B is reachable. (Details not shown.)

# Display detailed information about VRRP group 1 on Switch A.
[SwitchA] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode       : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
    VRID : 1         Adver Timer : 100
    Admin Status : Up         State : Backup
    Config Pri : 100         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

# Display detailed information about VRRP group 1 on Switch B.
[SwitchB] display vrrp verbose
IPv4 Virtual Router Information:
Running Mode       : Standard
Total number of virtual routers : 1
Interface Vlan-interface2
    VRID : 1         Adver Timer : 100
    Admin Status : Up         State : Master

272
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 Switch A becomes the backup, and Switch B becomes the master. Switch B forwards packets from Host A to Host B.

Static routing-Track-LLDP collaboration configuration example

Network requirements

As shown in Figure 66:

- Device A is the default gateway of the hosts in network 20.1.1.0/24.
- Device B is the default gateway of the hosts in network 30.1.1.0/24.
- Hosts in the two networks communicate with each other through static routes.

To ensure network availability, configure route backup and static routing-Track-LLDP collaboration on Device A and Device B as follows:

- On Device A, assign a higher priority to the static route to 30.1.1.0/24 with next hop Device B. This route is the master route. The static route to 30.1.1.0/24 with next hop Device C acts as the backup route. When the master route is unavailable, the backup route takes effect. Device A forwards packets destined for 30.1.1.0/24 to Device C.
- On Device B, assign a higher priority to the static route to 20.1.1.0/24 with next hop Device A. This route is the master route. The static route to 20.1.1.0/24 with next hop Device C acts as the backup route. When the master route is unavailable, the backup route takes effect. Device B forwards packets destined for 20.1.1.0/24 to Device C.

Figure 66 Network diagram

Configuration procedure

1. Configure the IP address of each interface, as shown in Figure 66. (Details not shown.)
2. Configure Device A:
   
   # Configure a static route to 30.1.1.0/24 with next hop 10.1.1.2 and the default priority (60). Associate this static route with track entry 1.
   
   <DeviceA> system-view
   [DeviceA] 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 next hop 10.3.1.3 and priority 80.
Configure Device A:

# Enable LLDP globally.
[DeviceA] lldp global enable

# Enable LLDP on GigabitEthernet 1/0/1. (This step is optional because LLDP is enabled on the port by default.)
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] lldp enable

# Configure track entry 1 and associate it with the availability of the neighbor for LLDP interface Gigabitethernet 1/0/1.
[DeviceA] track 1 lldp neighbor interface gigabitethernet 1/0/1

Configure Device B:

# Configure a static route to 20.1.1.0/24 with next hop 10.2.1.1 and the default priority (60). Associate this static route with track entry 1.
<DeviceB> system-view
[DeviceB] 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 next hop 10.4.1.3 and priority 80.
[DeviceB] ip route-static 20.1.1.0 24 10.4.1.3 preference 80

# Enable LLDP globally.
[DeviceB] lldp global enable

# Enable LLDP on the GigabitEthernet 1/0/1. (This step is optional because LLDP is enabled on the port by default.)
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] lldp enable

# Configure track entry 1 and associate it with the availability of the neighbor for LLDP interface Gigabitethernet 1/0/1.
[DeviceB] track 1 lldp neighbor interface gigabitethernet 1/0/1

Configure Device C:

# Configure a static route to 30.1.1.0/24 with next hop 10.4.1.2.
<DeviceC> system-view
[DeviceC] ip route-static 30.1.1.0 24 10.4.1.2

# Configure a static route to 20.1.1.0/24 with next hop 10.3.1.1.
[DeviceC] ip route-static 20.1.1.0 24 10.3.1.1

Verifying the configuration

# Display track entry information on Device A.
[DeviceA] display track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    LLDP interface: GigabitEthernet1/0/1

The output shows that the status of track entry 1 is Positive, indicating that the neighbor of LLDP interface GigabitEthernet 1/0/1 is available. The master route takes effect.

# Display the routing table of Device A.
[DeviceA] display ip routing-table

Destinations : 9      Routes : 9
### Destination/Mask and Routing Table

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>10.2.1.1</td>
<td>XGE1/1/1</td>
</tr>
<tr>
<td>10.2.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>10.3.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>10.3.1.1</td>
<td>XGE1/1/2</td>
</tr>
<tr>
<td>10.3.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>20.1.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>20.1.1.1</td>
<td>XGE1/1/3</td>
</tr>
<tr>
<td>20.1.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>30.1.1.0/24</td>
<td>Static</td>
<td>60</td>
<td>0</td>
<td>10.3.1.3</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
</tbody>
</table>

The output shows that Device A forwards packets to 30.1.1.0/24 through Device B.

# On Device B, disable LLDP on GigabitEthernet 1/0/1.

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo lldp enable
```

# Display track entry information on Device A.

```
[DeviceA] display track all
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    LLDP interface: GigabitEthernet1/0/1
```

The output shows that the status of track entry 1 is Negative, indicating that the neighbor of LLDP interface GigabitEthernet 1/0/1 is unavailable. The master route fails.

# Display the routing table of Device A.

```
[DeviceA] display ip routing-table
Destinations : 9  Routes : 9
```

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>10.2.1.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>10.2.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>10.3.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>10.3.1.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>10.3.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>20.1.1.0/24</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>20.1.1.1</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>20.1.1.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>30.1.1.0/24</td>
<td>Static</td>
<td>80</td>
<td>0</td>
<td>10.3.1.3</td>
<td>GE1/0/1</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>Direct</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoop0</td>
</tr>
</tbody>
</table>

The output shows that Device A forwards packets destined for 30.1.1.0/24 to Device C. The backup static route has taken effect.

# Verify that hosts in 20.1.1.0/24 can communicate with the hosts in 30.1.1.0/24 when the master route fails.

```
[DeviceA] ping -a 20.1.1.1 30.1.1.1
Ping 30.1.1.1: 56  data bytes, press CTRL_C to break
```
# Verify that the hosts in 30.1.1.0/24 can communicate with the hosts in 20.1.1.0/24 when the master route fails.

```
[DeviceB] 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
--- Ping statistics for 20.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms

Smart Link-Track-CFD collaboration configuration example

For information about the Smart Link-Track-CFD collaboration configuration example, see "Configuring Smart Link."

EVI IS-IS-Track-BFD collaboration configuration example

**Network requirements**

As shown in Figure 67:

- Use EVI to extend VLANs 21 through 100 across site 1, site 2, and site 3 over an IPv4 network.
- Deploy Switch A and Switch B to connect site 1 to the EVI network for redundancy. Use VLAN 2012 as the designated site VLAN.
- Use network ID 1 to identify the EVI network.
- Use Switch B as an ENDS and all other edge switches as ENDCs for neighbor discovery.
- Configure a track entry on Switch A and Switch B to monitor their respective EVI links to site 1 for quick failover.
Configuration procedure

1. Configure routes for the sites to reach each other. (Details not shown.)
2. Configure Switch A:

   # Configure the site ID.
   <SwitchA> system-view
   [SwitchA] evi site-id 1

   # Create VLAN 10, and assign the transport-facing physical interface GigabitEthernet 1/0/2 to the VLAN.
   [SwitchA] vlan 10
   [SwitchA-vlan10] port gigabitethernet 1/0/2
   [SwitchA-vlan10] quit

   # Create VLAN-interface 10, and assign an IP address to it.
   [SwitchA] interface vlan-interface 10
   [SwitchA-Vlan-interface10] ip address 1.1.1.1 24
   [SwitchA-Vlan-interface10] quit

   # Create an IPv4 EVI tunnel interface.
   [SwitchA] interface tunnel 1 mode evi

   # Specify the IP address of VLAN-interface 10 as the source IP of the EVI tunnel.
   [SwitchA-Tunnel1] source 1.1.1.1

   # Set the network ID to 1 for the EVI tunnel interface.
   [SwitchA-Tunnel1] evi network-id 1

   # Specify extended VLANs on the EVI tunnel interface.
   [SwitchA-Tunnel1] evi extend-vlan 21 to 100

   # Configure Switch A as an ENDC of Switch B.
   [SwitchA-Tunnel1] evi neighbor-discovery client enable 1.1.2.2
# Configure track entry 1 with BFD to monitor the link between Switch A and Switch C.
[SwitchA] bfd echo-source-ip 8.8.8.81
[SwitchA] track 1 bfd echo interface vlan-interface 10 remote ip 1.1.3.3 local ip 1.1.1.1

# Associate the EVI tunnel interface with track entry 1.
[SwitchA] interface tunnel 1
[SwitchA-Tunnel1] evi isis track 1
[SwitchA-Tunnel1] quit

# Configure VLAN 2012 as the designated EVI IS-IS site VLAN, and assign GigabitEthernet 1/0/1 to the VLAN.
[SwitchA] vlan 2012
[SwitchA-vlan2012] port gigabitethernet 1/0/1
[SwitchA-vlan2012] quit
[SwitchA] evi designated-vlan 2012

# Enable EVI on the transport-facing port GigabitEthernet 1/0/2.
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] evi enable
[SwitchA-GigabitEthernet1/0/2] quit

3. Configure Switch B:

# Configure the site ID.
<SwitchB> system-view
[SwitchB] evi site-id 1

# Create VLAN 10, and assign the transport-facing physical interface GigabitEthernet 1/0/2 to VLAN 10.
[SwitchB] vlan 10
[SwitchB-vlan10] port gigabitethernet 1/0/2
[SwitchB-vlan10] quit

# Create VLAN-interface 10, and assign an IP address to it.
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ip address 1.1.2.2 24
[SwitchB-Vlan-interface10] quit

# Create an IPv4 EVI tunnel interface.
[SwitchB] interface tunnel 1 mode evi

# Specify the IP address of VLAN-interface 10 as the source IP of the EVI tunnel.
[SwitchB-Tunnel1] source 1.1.2.2

# Set the network ID to 1 for the EVI tunnel interface.
[SwitchB-Tunnel1] evi network-id 1

# Specify extended VLANs on the EVI tunnel interface.
[SwitchB-Tunnel1] evi extend-vlan 21 to 100

# Configure Switch B as an ENDS on the EVI tunnel interface.
[SwitchB-Tunnel1] evi neighbor-discovery server enable

# Set a DED priority of 100 on the EVI tunnel interface.
[SwitchB-Tunnel1] evi isis ded-priority 100
[SwitchB-Tunnel1] quit

# Associate track entry 1 with BFD to monitor the link between Switch B and Switch C.
[SwitchB] bfd echo-source-ip 8.8.8.82
[SwitchB] track 1 bfd echo interface vlan-interface 10 remote ip 1.1.3.3 local ip 1.1.2.2

# Associate the EVI tunnel interface with track entry 1.
[SwitchB] interface tunnel 1
[SwitchB-Tunnel1] evi isis track 1
[SwitchB-Tunnel1] quit

# Configure VLAN 2012 as the designated EVI IS-IS site VLAN, and assign GigabitEthernet 1/0/1 to the VLAN.
[SwitchB] vlan 2012
[SwitchB-vlan2012] port gigabitethernet 1/0/1
[SwitchB-vlan2012] quit
[SwitchB] evi designated-vlan 2012

# Enable EVI on the transport-facing port GigabitEthernet 1/0/2.
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] evi enable
[SwitchB-GigabitEthernet1/0/2] quit

4. Configure Switch C:
   # Configure the site ID.
   <SwitchC> system-view
   [SwitchC] evi site-id 2

   # Create VLAN 10, and assign the transport-facing physical interface GigabitEthernet 1/0/2 to VLAN 10.
   [SwitchC] vlan 10
   [SwitchC-vlan10] port gigabitethernet 1/0/2
   [SwitchC-vlan10] quit

   # Create VLAN-interface 10, and assign an IP address to it.
   [SwitchC] interface vlan-interface 10
   [SwitchC-Vlan-interface10] ip address 1.1.3.3 24
   [SwitchC-Vlan-interface10] quit

   # Create an IPv4 EVI tunnel interface.
   [SwitchC] interface tunnel 1 mode evi

   # Specify the IP address of VLAN-interface 10 as the source IP of the EVI tunnel.
   [SwitchC-Tunnel1] source 1.1.3.3

   # Set the network ID to 1 for the EVI tunnel interface.
   [SwitchC-Tunnel1] evi network-id 1

   # Specify extended VLANs on the EVI tunnel interface.
   [SwitchC-Tunnel1] evi extend-vlan 21 to 100

   # Configure Switch C as an ENDC of Switch B.
   [SwitchC-Tunnel1] evi neighbor-discovery client enable 1.1.2.2
   [SwitchC-Tunnel1] quit

   # Enable EVI on the transport-facing port GigabitEthernet 1/0/2.
   [SwitchC] interface gigabitethernet 1/0/2
   [SwitchC-GigabitEthernet1/0/2] evi enable
   [SwitchC-GigabitEthernet1/0/2] quit

Verifying the configuration

1. Verify the configuration on Switch A:
   # Display neighbor entries that Switch A has learned.
[SwitchA] display evi neighbor-discovery client member
Interface: Tunnel1    Network ID: 1
Local Address: 1.1.1.1
Server Address: 1.1.2.2
Neighbor        System ID         Created Time           Expire    Status
1.1.2.2         c4ca-d94d-1385    2016/01/06 09:40:26    64        Up
1.1.3.3         c4ca-d94d-138d    2016/01/06 09:40:26    64        Up

# Display information about EVI-Link interfaces.
[SwitchA] display evi link interface tunnel 1
Interface     Status Source          Destination
EVI-Link0     UP     1.1.1.1         1.1.2.2
EVI-Link1     UP     1.1.1.1         1.1.3.3

# Display BFD session information.
[SwitchA] display bfd session
Total Session Num: 1     Up Session Num: 1     Init Mode: Active
IPv4 Session Working Under Echo Mode:

LD             SourceAddr      DestAddr        State    Holdtime    Interface 1025           1.1.1.1         1.1.3.3         Up       2331ms      Vlan10

The output shows that the BFD session on Switch A is up. This state indicates that the EVI link from Switch A to Switch C is operating correctly.

# Display EVI IS-IS information for the EVI tunnel interface. Check the DED field and the LAV field to verify the DED role and active extended VLANs on Switch A. Check the AEF field to verify the qualification of Switch A as an appointed edge forwarder.
[SwitchA] display evi isis tunnel 1
Tunnel1
MTU: 1400
DED: No
DED priority: 64
Hello timer: 10s
Hello multiplier: 3
CSNP timer: 10s
LSP timer: 100ms
LSP transmit-throttle count: 5
AEF: Yes
EVI-Link0    DED: Yes
EVI-Link1    DED: No
LAV: 61-100

The output shows that Switch A is not elected the DED for site 1 because of its low DED priority. Switch A can be an appointed edge forwarder for extended VLANs. VLAN 61 to VLAN 100 are active on Switch A.

2. Verify the configuration on Switch B:
# Display neighbor entries that Switch B has learned.
[SwitchB] display evi neighbor-discovery client member interface tunnel 1
Interface: Tunnel1    Network ID: 1
Local Address: 1.1.2.2
Server Address: 1.1.2.2
Neighbor        System ID         Created Time           Expire    Status
1.1.1.1         c4ca-d94d-1200    2016/01/06 09:40:30    74        Up
1.1.3.3         c4ca-d94d-138d    2016/01/06 09:40:15    74        Up

# Display EVI neighbors registered with the ENDS.
[SwitchB] display evi neighbor-discovery server member interface tunnel 1
Interface: Tunnel1    Network ID: 1
IP Address: 1.1.2.2
Client Address  System ID         Expire    Created Time
1.1.1.1         c4ca-d94d-1200    64        2016/01/06 09:40:16
1.1.2.2         c4ca-d94d-1385    68        2016/01/06 09:32:00
1.1.3.3         c4ca-d94d-138d    67        2016/01/06 09:40:14

# Display information about EVI-Link interfaces.
[SwitchB] display evi link interface tunnel 1
Interface     Status Source          Destination
EVI-Link0     UP     1.1.2.2         1.1.1.1
EVI-Link1     UP     1.1.2.2         1.1.3.3

# Display BFD session information.
[SwitchB] display bfd session
Total Session Num: 1     Up Session Num: 1     Init Mode: Active
IPv4 Session Working Under Echo Mode:

<table>
<thead>
<tr>
<th>LD</th>
<th>SourceAddr</th>
<th>DestAddr</th>
<th>State</th>
<th>Holdtime</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1025</td>
<td>1.1.2.2</td>
<td>1.1.3.3</td>
<td>Up</td>
<td>2055ms</td>
<td>Vlan10</td>
</tr>
</tbody>
</table>

The output shows that the BFD session on Switch B is up. This state indicates that the EVI link from Switch B to Switch C is operating correctly.

# Display EVI IS-IS information for the EVI tunnel interface. Check the DED field and the LAV field to verify the DED role and active extended VLANs on Switch B. Check the AEF field to verify the qualification of Switch B as an appointed edge forwarder.
[SwitchB] display evi isis tunnel 1
Tunnel1
MTU: 1400
DED: Yes
DED priority: 100
Hello timer: 10s
Hello multiplier: 3
CSNP timer: 10s
LSP timer: 100ms
LSP transmit-throttle count: 5
AEF: Yes
EVI-Link0    DED: Yes
EVI-Link1    DED: Yes
LAV:        21-60

The output shows that Switch B is elected the DED for site 1 because of its high DED priority. Switch B can be an appointed edge forwarder for extended VLANs. VLAN 21 to VLAN 60 are active on Switch B.

3. Verify the configuration on Switch C:
# Display neighbor entries that Switch C has learned.

```
[SwitchC] display evi neighbor-discovery client member
Interface: Tunnel1    Network ID: 1
Local Address: 1.1.3.3
Server Address: 1.1.2.2
```

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>System ID</th>
<th>Created Time</th>
<th>Expire</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>c4ca-d94d-1200</td>
<td>2016/01/06 09:40:29</td>
<td>64</td>
<td>Up</td>
</tr>
<tr>
<td>1.1.2.2</td>
<td>c4ca-d94d-1385</td>
<td>2016/01/06 09:40:29</td>
<td>64</td>
<td>Up</td>
</tr>
</tbody>
</table>

# Display information about EVI-Link interfaces.

```
[SwitchC] display evi link interface tunnel 1
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVI-Link0</td>
<td>UP</td>
<td>1.1.3.3</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>EVI-Link1</td>
<td>UP</td>
<td>1.1.3.3</td>
<td>1.1.2.2</td>
</tr>
</tbody>
</table>

4. Verify that hosts in different sites can ping one another in the same extended VLAN.

5. Verify that a failover occurs immediately after BFD detects an EVI link failure on Switch B.

# Display BFD session information on Switch A.

```
[SwitchA] display bfd session
```

IPv4 Session Working Under Echo Mode:

```
LD   SourceAddr   DestAddr   State   Holdtime   Interface
1025 1.1.1.1      1.1.3.3    Up       2330ms      Vlan10
```

The output shows that the BFD session on the EVI link between Switch A and Switch C is up. The EVI link on Switch A is operating correctly.

# Display BFD session information on Switch B.

```
[SwitchB] display bfd session
```

IPv4 Session Working Under Echo Mode:

```
LD   SourceAddr   DestAddr   State   Holdtime   Interface
1025 1.1.2.2      1.1.3.3    Down     /          Vlan10
```

The output shows that the BFD session on the EVI link between Switch B and Switch C is down. This state indicates that the EVI link has failed.

# On Switch A, verify that all active VLANs on Switch B have been moved to Switch A after the EVI link on Switch B fails.

```
[SwitchA] display evi isis tunnel 1
```

Tunnel1
MTU: 1400
DED: No
DED priority: 64
Hello timer: 10s
Hello multiplier: 3
CSNP timer: 10s
LSP timer: 100ms
LSP transmit-throttle count: 5
AEF: Yes
EVI-Link0    DED: Yes
EVI-Link1    DED: No

LAV:
  21-100

# Verify that the appointed edge forwarder role of Switch B has been removed because it is
down, and the switch does not have any active VLANs.

[SwitchB] display evi isis tunnel 1
Tunnel1
MTU: 1400
DED: Yes
DED priority: 100
Hello timer: 10s
Hello multiplier: 3
CSNP timer: 10s
LSP timer: 100ms
LSP transmit-throttle count: 5
AEP: No
EVI-Link0    DED: Yes
LAV:
  None
Configuring process placement

Overview

Process placement enables placing processes to specific CPUs (also called nodes) on the main processing units (MPUs) in your system for optimal distribution of CPU and memory resources.

Process

A process contains a set of codes and provides specific functionality. For example, an AAA process provides AAA functions.

Each process runs in a protected memory space to prevent problems with one process from impacting the entire system.

1:N process redundancy

The system backs up each active process running on one node to all the other nodes. When an active process fails, one of its standby processes promptly takes over without impacting any other service.

1:N process redundancy provides the following benefits:

- Improves service availability.
- Enables the system to quickly regain reliability after device status changes in such conditions as insertion and removal of cards, IRF split, and removal of an IRF member.

Process placement policy and optimization

Process placement policies

(In standalone mode.) The execution of process placement policies varies by the location of active processes.

- An active process running only on the active MPU does not support placement optimization. If you configure a process placement policy for the process, the system displays a configuration failure prompt. When such an active process fails, the system automatically restarts the process. The standby processes are used for active/standby switchover and ISSU.
- Some active processes can run on either the active or standby MPU. When such an active process fails, the system uses a placement policy to select a new active process among standby processes.

(In IRF mode.) The execution of process placement policies varies by the location of active processes.

- An active process running only on the global active MPU does not support placement optimization. If you configure a process placement policy for the process, the system displays a configuration failure prompt. When such an active process fails, the system automatically restarts the process. The standby processes are used for active/standby switchover and ISSU.
- Some active processes can run on either the global active or standby MPU. When such an active process fails, the system uses a placement policy to select a new active process among standby processes.

The system provides a default process placement policy that takes effect for all processes. You can modify the default placement policy in the view you enter by using the placement program default command. You can also configure a placement policy for a specific process in the view you enter by
using the placement program program-name [ instance instance-name ] command. A placement policy for a process takes precedence over the default process placement policy.

By default, the default process placement policy defines the following rules:

- (In standalone mode.) The active process runs on the main CPU of the active MPU, and the standby processes run on the main CPU of the standby MPU.
- (In IRF mode.) The active process runs on the main CPU of the global active MPU, and the standby processes run on the main CPU of the global standby MPU.
- A process runs at the location where it ran the last time and does not move to any other location during startup or operation.
- The addition of a new node does not impact current active processes. A new active process selects one node with sufficient CPU and memory resources. (You can use the display cpu-usage and display memory commands to view CPU and memory usage information.)

Optimizing process placement

You can configure the following settings for a process placement policy to optimize process placement:

- **affinity location-set**—Location affinity, the preference for the process to run on a specific node.
- **affinity location-type**—Location type affinity, the preference for the process to run on a particular type of node. For more information about node types, see "Configuring a location type affinity."
- **affinity program**—Process affinity, the preference for the process to run on the same node as a particular process.
- **affinity self**—Self affinity, the preference for one instance of the process to run on the same node as any other instance of the process.

Affinities include positive affinities (attract) and negative affinities (repulse), all represented by integers in the range of 1 to 100000.

- The higher the attract value, the stronger the preference.
- The higher the repulse value, the weaker the preference.

After you apply new placement policies, the system makes placement decisions based on the new policies, node resources, and topology status. If the new location for an active process is different from the current node, the system changes the state of the process to standby, and uses the standby process on the preferred location as the new active process.

Configuration restrictions and guidelines

When you configure process placement, follow these restrictions and guidelines:

- Configuring process placement on a device with only one MPU does not change the location of processes. All processes run on the main CPU of the MPU.
- Configuring process placement on a device with multiple MPUs places specific active processes to specific CPUs. In case of multiple CPUs, the system performs 1:N process redundancy. The number of standby processes and their CPU locations vary by function module. The system by default automatically determines the location for each active process, and process placement optimization is not required. If optimization is required, contact Hewlett Packard Enterprise Support to avoid service interruption.
- Do not perform process placement for a process frequently.
- Process placement applies only to MPUs.
- To view the current location of an active process and its predicted new location after optimization, use the display placement reoptimize command.
Process placement configuration task list

Tasks at a glance

Configuring process placement policy:
- (Optional.) Configuring a location affinity
- (Optional.) Configuring a location type affinity
- (Optional.) Configuring a process affinity
- (Optional.) Configuring a self affinity

(Required.) Optimizing process placement

Configuring process placement policy

Configuring a location affinity

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter placement process view. | • Enter default placement process view: placement program default
• Enter placement process view: placement program { program-name [ instance instance-name ]} | Settings in default placement process view take effect for all processes. Settings in placement process view take effect only for the specified process. |
| 3.   | Set the location affinity. | • In standalone mode: affinity location-set slot slot-number&<1-5> { attract strength | default | none | repulse strength }
• In IRF mode: affinity location-set chassis chassis-number slot slot-number&<1-5> { attract strength | default | none | repulse strength } | By default, no location affinity is set. |

Configuring a location type affinity

The following location types are available:
- **current**—Current location of the active process, which can be displayed with the **display placement program** command.
- **paired**—Locations of standby processes.
- (In standalone mode.) **primary**—Active MPU.
- (In IRF mode.) **primary**—Global active MPU.

To configure a location type affinity:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
### Configuring a process affinity

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter placement process view.</td>
<td>placement program default</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the affinity for the process to run on the same location as another process.</td>
<td>affinity program program-name { attract strength</td>
</tr>
</tbody>
</table>

### Configuring a self affinity

Perform this task to configure the preference for one instance of a process to run on the same node as any other instance of the process. The self affinity setting does not take effect for a process that has only one instance.

To configure a self affinity:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter placement process view.</td>
<td>placement program default</td>
</tr>
<tr>
<td>3.</td>
<td>Configure a self affinity.</td>
<td>affinity self { attract strength</td>
</tr>
</tbody>
</table>
## Optimizing process placement

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
</tbody>
</table>
| 2.   | Optimize process placement. | `placement reoptimize`  
To keep the system stable, do not perform any tasks that require process restart when you execute this command. |

## Displaying process placement

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display process placement policy information.</td>
<td>`display placement policy program { program-name</td>
</tr>
<tr>
<td>Display the location of a process.</td>
<td>`display placement program { program-name</td>
</tr>
<tr>
<td>(In standalone mode.) Display the running processes on a specific location.</td>
<td>`display placement location { slot slot-number</td>
</tr>
<tr>
<td>(In IRF mode.) Display the running processes on a specific location.</td>
<td>`display placement location { chassis chassis-number slot slot-number</td>
</tr>
<tr>
<td>Display the predicted location of a process after process placement optimization.</td>
<td>`display placement reoptimize program { program-name [ instance instance-name ]</td>
</tr>
<tr>
<td>Display service group information.</td>
<td>`display ha service-group { program-name [ instance instance-name ]</td>
</tr>
</tbody>
</table>
Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Command conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Bold text represents commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td><em>Italic</em> text represents arguments that you replace with actual values.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square brackets enclose syntax choices (keywords or arguments) that are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>&amp;&lt;1-n&gt;</td>
<td>The argument or keyword and argument combination before the ampersand (&amp;) sign can be entered 1 to n times.</td>
</tr>
<tr>
<td>#</td>
<td>A line that starts with a pound (#) sign is comments.</td>
</tr>
</tbody>
</table>

GUI conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Window names, button names, field names, and menu items are in Boldface. For example, the New User window opens; click OK.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Multi-level menus are separated by angle brackets. For example, File &gt; Create &gt; Folder.</td>
</tr>
</tbody>
</table>

Symbols

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶️ WARNING!</td>
<td>An alert that calls attention to important information that if not understood or followed can result in personal injury.</td>
</tr>
<tr>
<td>▶️ CAUTION:</td>
<td>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.</td>
</tr>
<tr>
<td>☑️ IMPORTANT:</td>
<td>An alert that calls attention to essential information.</td>
</tr>
<tr>
<td>✑️ NOTE:</td>
<td>An alert that contains additional or supplementary information.</td>
</tr>
<tr>
<td>💡 TIP:</td>
<td>An alert that provides helpful information.</td>
</tr>
</tbody>
</table>
# Network topology icons

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Represents a generic network device, such as a router, switch, or firewall.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Represents a routing-capable device, such as a router or Layer 3 switch.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>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.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Represents an access point.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Represents a wireless terminator unit.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Represents a wireless terminator.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Represents a mesh access point.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Represents omnidirectional signals.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Represents directional signals.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.</td>
</tr>
</tbody>
</table>

## Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.
Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
  [www.hpe.com/assistance](http://www.hpe.com/assistance)
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
  [www.hpe.com/support/hpesc](http://www.hpe.com/support/hpesc)

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center [Get connected with updates](http://www.hpe.com/support/e-updates) page:
    [www.hpe.com/support/e-updates](http://www.hpe.com/support/e-updates)
  - Software Depot website:
    [www.hpe.com/support/softwaredepot](http://www.hpe.com/support/softwaredepot)
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center [More Information on Access to Support Materials](http://www.hpe.com/support/AccessToSupportMaterials) page:

**IMPORTANT:**

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.
Websites

<table>
<thead>
<tr>
<th>Website</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking websites</td>
<td></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Information Library for Networking</td>
<td><a href="http://www.hpe.com/networking/resourcefinder">www.hpe.com/networking/resourcefinder</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Networking website</td>
<td><a href="http://www.hpe.com/info/networking">www.hpe.com/info/networking</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise My Networking website</td>
<td><a href="http://www.hpe.com/networking/support">www.hpe.com/networking/support</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Networking Warranty</td>
<td><a href="http://www.hpe.com/networking/warranty">www.hpe.com/networking/warranty</a></td>
</tr>
<tr>
<td>General websites</td>
<td></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Information Library</td>
<td><a href="http://www.hpe.com/info/enterprise/docs">www.hpe.com/info/enterprise/docs</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Support Center</td>
<td><a href="http://www.hpe.com/support/hpesc">www.hpe.com/support/hpesc</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Support Services Central</td>
<td>ssc.hpe.com/portal/site/ssc/</td>
</tr>
<tr>
<td>Contact Hewlett Packard Enterprise Worldwide</td>
<td><a href="http://www.hpe.com/assistance">www.hpe.com/assistance</a></td>
</tr>
<tr>
<td>Subscription Service/Support Alerts</td>
<td><a href="http://www.hpe.com/support/e-updates">www.hpe.com/support/e-updates</a></td>
</tr>
<tr>
<td>Software Depot</td>
<td><a href="http://www.hpe.com/support/softwaredepot">www.hpe.com/support/softwaredepot</a></td>
</tr>
<tr>
<td>Customer Self Repair (not applicable to all devices)</td>
<td><a href="http://www.hpe.com/support/selfrepair">www.hpe.com/support/selfrepair</a></td>
</tr>
<tr>
<td>Insight Remote Support (not applicable to all devices)</td>
<td><a href="http://www.hpe.com/info/insightremotesupport/docs">www.hpe.com/info/insightremotesupport/docs</a></td>
</tr>
</tbody>
</table>

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website: www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product’s service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website: www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title,
part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.
Index

Numerics
1:N process redundancy, 284
1-way DM
   CFD 1-way DM configuration, 26
2-way DM
   CFD 2-way DM configuration, 26
A
action
   Ethernet OAM port action, 11
activating RRPP domain, 64
active
   switchover (high availability technologies), 2
   virtual forwarder. Use AVF
advertising
   high availability DLDP advertisement packet send interval, 39
   high availability DLDP advertisement timer, 35
   VRRP advertisement interval, 177
affinity
   process placement affinity (location type), 286
   process placement affinity (location), 286
   process placement affinity (process), 287
   process placement affinity (self), 287
   process placement location-set, 285
   process placement location-type, 285
   process placement negative (repulse) affinity, 285
   process placement positive (attract) affinity, 285
   process placement program, 285
   process placement self, 285
AIS
   CFD AIS configuration, 25
   CFD function, 19
application
   NQA+Track+static routing collaboration, 238
   Track+application module association, 242
   Track+EAA association, 249
   Track+ERPS association, 249
   Track+EVI IS-IS association, 246
   Track+MPLS L2VPN association, 248
   Track+policy-based routing association, 244
   Track+Smart Link association, 245
   Track+static routing association, 243
   Track+VPLS association, 247
   Track+VRRP association, 242
   Track+VRRP group association, 243
   Track+VRRP VF association, 243
   Track+VXLAN association, 247
   VRRP, 178
   VRRP load-sharing, 179
   VRRP master/backup, 178
application scenario
   redundant Ethernet (Reth) interface, 228
ARP
   VRRP virtual MAC address assignment, 180
assigning
   IPv4 VRRP virtual IP address, 185
   IPv6 VRRP virtual IP address, 192
   VRRP virtual MAC address assignment, 180
assistant edge node
   specifying RRPP, 64
assistant-edge node
   RRPP type, 53
associating
   Smart Link associated device, 151
   Track+ERPS, 249
   Track+application module, 242
   Track+BFD, 239
   Track+CFD, 240
   Track+detection modules, 239
   Track+EAA, 249
   Track+EVI IS-IS association, 246
   Track+interface management, 240
   Track+LLDP, 241
   Track+MPLS L2VPN, 248
   Track+NQA, 239
   Track+policy-based routing, 244
   Track+route management, 241
   Track+Smart Link, 245
   Track+static routing, 243
   Track+VPLS, 247
   Track+VRRP, 242
   Track+VRRP group, 243
   Track+VRRP VF, 243
   Track+VXLAN, 247
attribute
   IPv4 VRRP packet attribute, 187
   IPv6 VRRP packet attribute, 195
authenticating
   high availability DLDP MD5 authentication, 40
   high availability DLDP MD5 mode, 36
high availability DLDP non-authentication mode, 36
high availability DLDP password authentication, 40
high availability DLDP plaintext authentication, 40
high availability DLDP plaintext mode, 36
high availability DLDP simple authentication, 40
VRRP MD5 authentication, 176
VRRP simple authentication, 176
auto
CFD MIP auto-generation rule, 22
automatic
high availability DLDP automatic unidirectional link shutdown, 41
AVF
VRRP virtual forwarder (VF) weight/priority, 182
B
backing up
Smart Link backup, 146
Track+EAA association, 249
Track+ERPS association, 249
Track+MPLS L2VPN association, 248
Track+VXLAN association, 247
VRRP virtual forwarder (VF) backup, 182
BFD
basic configuration, 234
configuration, 21
configuration restrictions, 234
display, 236
echo packet mode configuration, 234
EVI IS-IS+Track+BFD collaboration, 276
high availability fault detection technologies, 2
maintain, 236
multihop detection, 232
protocols and standards, 233
session and operating modes, 232
session establishment and termination, 232
single-hop detection, 232
SNMP notification enable, 236
static routing+Track+BFD collaboration, 264
supported features, 233
Track BFD+VRRP backup master monitor, 254
Track BFD+VRRP master uplink monitor, 256
Track+BFD association, 239
VRRP tracking, 178
forwarding detection. Use BFD
high availability DLDP port state, 35
broadcast (RRPP storm suppression mechanism), 56
C
calculating
MTBF, 1
MTTR, 1
CFD
1-way DM configuration, 26
2-way DM configuration, 26
AIS configuration, 25
basic concepts, 16
basic configuration, 21
configuration, 16, 20, 28
configuration restrictions, 20
display, 27
continuity check configuration, 23
eAIS configuration, 27
enable, 21
Ethernet alarm indication signal (EAIS) function, 20
Ethernet service instance configuration, 21
function configuration, 23
functions, 18
linktrace (LT) configuration, 24
LM configuration, 25
loopback (LB) configuration, 24
maintain, 27
MEP configuration, 22
MIP auto-generation rule, 22
protocols and standards, 20
Smart Link+Track+CFD collaboration, 276
Track+CFD association, 240
TST configuration, 26
collaborating
EVI IS-IS+Track+BFD configuration, 276
NQA+Track+static routing collaboration, 238
Smart Link, 147
Smart Link+Monitor Link, 147
Smart Link+Track, 147, 151
Smart Link+Track+CFD collaboration, 276
static routing+Track+BFD collaboration, 264
static routing+Track+LLDP collaboration, 273
static routing+Track+NQA collaboration, 260
Track BFD+VRRP backup master monitor, 254
Track BFD+VRRP master uplink monitor, 256
Track configuration, 237, 238, 250
Track+application modules, 237
Track+detection modules, 237
VRRP+Track+interface management collaboration, 267
VRRP+Track+NQA collaboration, 250
VRRP+Track+route management collaboration, 270
common port (RRPP), 53
common-flush-FDB RRPPDU type, 54
complete-flush-FDB RRPPDU type, 54
configuration
ERPS ring, 105
one-ring ERPS, 112
configuring
associated rings for subrings, 110
BFD, 232
BFD basic functions, 234
BFD control packet mode, 235
BFD echo packet mode, 234
CFD, 16, 20, 28
CFD 1-way DM, 26
CFD 2-way DM, 26
CFD AIS, 25
CFD basic settings, 21
CFD continuity check, 23
CFD EAIS, 27
CFD Ethernet service instance, 21
CFD functions, 23
CFD linktrace (LT), 24
CFD LM, 25
CFD loopback (LB), 24
CFD MEP, 22
CFD MIP auto-generation rule, 22
CFD TST, 26
control VLANs, 107
DLDP, 34
DLDP hybrid mode, 48
ERPS, 96, 112
ERPS (1 ring multi-instance load balancing), 134
ERPS (1 subring), 120
ERPS ring, 105
Ethernet OAM, 4, 7, 14
Ethernet OAM basics, 7
Ethernet OAM connection detection timer, 7
Ethernet OAM errored frame event detection, 9
Ethernet OAM errored frame period event detection, 10
Ethernet OAM errored seconds period event detection, 10
Ethernet OAM errored symbol event detection, 8
Ethernet OAM link monitoring, 8
Ethernet OAM port action, 11
Ethernet OAM remote loopback, 12
EVI IS-IS+Track+BFD collaboration, 276
high availability DLDL, 38, 41
high availability DLDL authentication, 40
high availability DLDL automatic unidirectional link shutdown, 41
IPv4 VRRP, 184, 197
IPv4 VRRP load balancing, 203
IPv4 VRRP master group following, 190
IPv4 VRRP multiple groups, 200
IPv4 VRRP packet attributes, 187
IPv4 VRRP router preemptive mode, 186
IPv4 VRRP router priority, 186
IPv4 VRRP router tracking function, 186
IPv4 VRRP single group, 197
IPv6 VRRP, 191, 211
IPv6 VRRP load balancing, 218
IPv6 VRRP master group following, 196
IPv6 VRRP multiple groups, 214
IPv6 VRRP packet attributes, 195
IPv6 VRRP router preemptive mode, 193
IPv6 VRRP router priority, 193
IPv6 VRRP router tracking function, 193
IPv6 VRRP single group, 211
Monitor Link, 167, 168, 170
Monitor Link group downlink interface switchover delay, 170
Monitor Link group member interface, 169
Monitor Link group member interface (group view), 169
Monitor Link group member interface (interface view), 169
node role, 108
process placement, 284, 286
process placement policy, 286
process placement policy affinity (location type), 286
process placement policy affinity (location), 286
process placement policy affinity (process), 287
process placement policy affinity (self), 287
protected VLANs, 107
R-APS packet levels, 109
redundant Ethernet (Reth) interface, 228, 229, 230
RRPP, 52, 60, 66
RRPP control VLAN, 60
RRPP dual-homed rings, 75
RRPP fail timer, 65
RRPP hello timer, 65
RRPP intersecting rings, 69
RRPP load-balanced intersecting rings, 85
RRPP node, 63
RRPP port, 62
RRPP protected VLAN, 61
RRPP ring, 62
RRPP ring group, 65
RRPP single ring, 66
Smart Link, 145, 148, 152
Smart Link associated device, 151
Smart Link device, 148
Smart Link group (multiple group load sharing), 157
Smart Link group (single group), 152
Smart Link group member port (group view), 149
Smart Link group member port (interface view), 150
Smart Link group protected VLAN, 148
Smart Link group role preemption mode, 150
Smart Link+Track collaboration, 151, 161
Smart Link+Track+CFD collaboration, 276
static routing+Track+BFD collaboration, 264
static routing+Track+LLDP collaboration, 273
static routing+Track+NQA collaboration, 260
Track, 237, 238, 250
Track BFD+VRRP backup master monitor, 254
Track BFD+VRRP master uplink monitor, 256
VRRP, 175
VRRP virtual forwarder (VF) tracking, 188
VRRP virtual forwarder tracking (VF), 194
VRRP+Track+interface management collaboration, 267
VRRP+Track+NQA collaboration, 250
VRRP+Track+route management collaboration, 270
confirmed DLDP neighbor state, 35
connecting
Ethernet OAM connection detection timer, 7
Ethernet OAM connection establishment, 5
Connectivity Fault Detection. Use CFD
continuity check
CFD configuration, 23
continuity check (CC)
CFD function, 18
control VLAN
RRPP, 53
RRPP configuration, 60
controlling
BFD control packet mode, 235
CPU
process placement configuration, 284, 286
creating
IPv4 VRRP group, 185
IPv6 VRRP group, 192
Monitor Link group, 168
RRPP domain, 60
D
default
CFD MIP default rule, 17
DelayDown timer (DLDP), 35, 39
detecting
BFD configuration, 232
DLDP configuration, 34
DLDP manual unidirectional link shutdown, 44
Ethernet OAM connection detection timer, 7
Ethernet OAM errored frame event detection, 9
Ethernet OAM errored frame period event detection, 10
Ethernet OAM errored frame seconds event detection, 10
Ethernet OAM errored symbol event detection, 8
Ethernet OAM remote fault detection, 6
high availability DLDP automatic unidirectional link shutdown, 41
high availability DLDP configuration, 38, 41
high availability DLDP multiple neighbors detection, 38
high availability DLDP single neighbor detection, 36
high availability fault detection technologies, 2
high availability protection switchover technologies, 2
NQA+Track+static routing collaboration, 238
Track configuration, 237
Track+application module collaboration, 237
Track+BFD association, 239
Track+CFD association, 240
Track+detection module association, 239
Track+detection module collaboration, 237
Track+interface management association, 240
Track+LLDP association, 241
Track+NQA association, 239
Track+route management association, 241
device
activating RRPP domain, 64
creating RRPP domain, 60
Device Link Detection Protocol. Use DLDP
DLDP configuration, 34
DLDP manual unidirectional link shutdown, 44
Ethernet OAM basic configuration, 7
Ethernet OAM configuration, 4, 7, 14
EVI IS-IS+Track+BFD collaboration, 276
high availability DLDp automatic unidirectional link shutdown, 41
high availability DLDp configuration, 38, 41
IPv4 VRRP configuration, 197
IPv4 VRRP load balancing configuration, 203
IPv4 VRRP multiple groups configuration, 200
IPv4 VRRP router preemptive mode, 186
IPv4 VRRP router priority, 186
IPv4 VRRP router tracking, 186
IPv4 VRRP single group configuration, 197
IPv6 VRRP configuration, 211
IPv6 VRRP load balancing configuration, 218
IPv6 VRRP multiple groups configuration, 214
IPv6 VRRP router preemptive mode, 193
IPv6 VRRP router priority, 193
IPv6 VRRP router tracking function, 193
IPv6 VRRP single group configuration, 211
Monitor Link configuration, 167, 168, 170
Monitor Link group creation, 168
Monitor Link group downlink interface switchover delay, 170
Monitor Link group member interface, 169
Monitor Link group uplink interface switchover threshold, 170
process placement configuration, 284, 286
Smart Link associated device, 151
Smart Link device, 148
Smart Link+Track+CFD collaboration, 276
static routing+Track+BFD collaboration, 264
static routing+Track+LLDP collaboration, 273
static routing+Track+NQA collaboration, 260
Track BFD+VRRP backup master monitor, 254
Track BFD+VRRP master uplink monitor, 256
Track configuration, 250
VRRP group router priority, 176
VRRP router preemption modes, 176
VRRP tracking, 178
VRRP+Track+interface management collaboration, 267
VRRP+Track+NQA collaboration, 250
VRRP+Track+route management collaboration, 270

disabling
IPv4 VRRP group, 191
IPv6 VRRP group, 197
disconnect state (RRPP ring), 53
displaying
BFD, 236
CFD, 27
ERPS, 111
Ethernet OAM, 13
high availability DLDp, 40
IPv4 VRRP, 191
IPv6 VRRP, 197
Monitor Link, 170
process placement, 288
redundant Ethernet (Reth) interface, 229
RRPP, 66
Smart Link, 152
Track entries, 250

DLDP
advertisement packet send interval, 39
authentication configuration, 40
authentication modes, 36
automatic unidirectional link shutdown, 41
basic concepts, 35
configuration, 34, 38, 41
configuration restrictions, 38
DelayDown timer, 39
displaying, 40
enabling, 39
high availability fault detection technologies, 2
how it works, 36
hybrid mode configuration, 48
maintaining, 40
manual unidirectional link shutdown, 44
multiple neighbors detection, 38
neighbor states, 35
port shutdown mode, 39
port states, 35
single neighbor detection, 36
timers, 35

DM
CFD function, 19
domain
activating (RRPP), 64
CFD maintenance domain, 16
creating (RRPP), 60
RRPP, 52
downlink
Monitor Link group downlink interface switchover delay, 170
dual-homed rings
RRPP configuration, 75
RRPP network, 58

E
Embedded Automation Architecture (EAA) Track association, 249

EAA Track+EAA association, 249

EAIS configuration, 27

CFD EAIS configuration, 27

CFD Ethernet alarm indication signal, 20

edge echo BFD echo packet mode, 234

high availability DLDL echo timer, 35

echo RRPPDU type, 54

RRPP node type, 53

RRPP port type, 53

specifying RRPP node, 64

electing VRRP master election, 177

Embedded Automation Architecture (EAA) Use EAA enabling BFD SNMP notifications, 236

CFD, 21

Ethernet OAM remote loopback for port (in port view), 13

Ethernet OAM remote loopback for port (in system view), 12

flush packet transparent transmission, 105

global ERPS, 104

high availability DLDL, 39

IPv4 VRRP gratuitous ARP packet periodic send, 189

IPv6 VRRP ND periodic packet send, 195

RRPP SNMP notification, 66

Smart Link flush message reception, 151

Smart Link flush message send, 150

VRRP SNMP notification, 191

enhanced timer (DLDL), 35

echo timer (DLDL), 35

ERPS 1 ring multi-instance load balancing configuration, 134

1 subring configuration, 120

configuration, 96, 112

configuration prerequisites, 104

configuration task list, 103

configuring control VLANs, 107

configuring ERPS ring, 105

configuring node role, 108

configuring one-ring ERPS, 112

configuring protected VLANs, 107

displaying, 111

enabling ERPS for instance, 108

enabling ERPS globally, 104

enabling R-APS packets to carry the ring ID in the destination MAC address, 105

ERPS ring member ports, 96

instances, 97

link detection and association mechanism, 100

link recovery mechanism, 99

link-down report mechanism, 99

maintaining, 111

manual configuration mechanism, 100

multi-instance and load balancing mechanism, 100

network diagrams, 101
	node states, 98

nodes, 96

one major ring connecting multiple subring network diagrams, 101

one major ring connecting one subring network diagrams, 101

one major ring network diagrams, 101

one subring connecting multiple ring network diagrams, 102

one subring connecting multiple subring network diagrams, 102

operation mechanism, 99

protocol packets, 97

ring mode setting removal, 111

ring structure, 96

timers, 98

Track association, 249

troubleshoot master node cannot receive SF packets, 144

ERPS configuration prerequisites, 104

task list, 103

ERPS instance port associating with a track entry, 111

ERPS network diagram one major ring connecting multiple subring network, 101

one major ring connecting one subring network, 101

one major ring network, 101

one subring connecting multiple ring network, 102

one subring connecting multiple subring network, 102

ERPS ring configuration, 105

ERPS ring ID destination MAC address, 105

ERPS ring member port configuration, 105, 106
ERPS ring member port attribute configuration, 106
ERPS setting timers, 109
ERPS subring associated ring configuration, 110
errored Ethernet OAM errored frame event detection, 9
Ethernet OAM errored frame period event detection, 10
Ethernet OAM errored frame seconds event detection, 10
Ethernet OAM errored symbol event detection, 8
establishing BFD session, 232
Ethernet OAM connection, 5
Ethernet CFD Ethernet alarm indication signal (EAIS), 20
link aggregation (protection switchover technologies), 2
OAM. Use Ethernet OAM redundant Ethernet (Reth) interface configuration, 228, 229, 230
ring protection switching. Use ERPS RRPP configuration, 52, 60, 66
RRPP dual-homed rings configuration, 75
RRPP intersecting rings configuration, 69
RRPP load-balanced intersecting rings configuration, 85
RRPP single ring configuration, 66
Ethernet OAM basic configuration, 7
configuration, 4, 7, 14
connection detection timer, 7
connection establishment, 5
display, 13
errored frame event detection, 9
errored frame period event detection, 10
errored frame seconds event detection, 10
errored symbol event detection, 8
functions, 4
high availability fault detection technology, 2
how it works, 4
link monitoring, 5
link monitoring configuration, 8
maintain, 13
OAMPDUs, 4
port action configuration, 11
protocols and standards, 6
remote fault detection, 6
remote loopback, 6
remote loopback configuration, 12
remote loopback configuration restrictions, 12
remote loopback for port (in port view), 13
remote loopback for port (in system view), 12
remote loopback request rejection, 13
evaluating network availability, 1
event Ethernet OAM errored frame event detection, 9
Ethernet OAM errored frame period event detection, 10
Ethernet OAM errored frame seconds event detection, 10
Ethernet OAM errored symbol event detection, 8
EVI IS-IS+Track+BFD collaboration, 276
Track+EVI IS-IS association, 246
explicit rule (CFD MIP), 17
F fail timer (RRPP), 55
fast BFD fast failure detection, 232
fault CFD basic configuration, 21
CFD configuration, 16, 20, 28
CFD functions, 18
CFD maintenance domain, 16
Ethernet OAM functions, 4
Ethernet OAM remote fault detection, 6
fault detection BFD basic configuration, 234
BFD configuration, 232
high availability protection switchover technologies, 2
high availability technologies, 2, 2
flush packet transparent transmission enabling, 105
flushing Smart Link flush message, 146
Smart Link flush message reception, 151
Smart Link flush message send, 150
Smart Link flush update, 147
forwarding bidirectional detection. Use BFD VRRP virtual forwarder (VF), 182
VRRP virtual forwarder (VF) tracking, 188
VRRP virtual forwarder tracking (VF), 194
G
GR (high availability protection switchover technology), 2
gratuitous ARP
    IPv4 VRRP gratuitous ARP packet periodic send, 189

group
    configuring RRPP ring, 65
    IPv4 VRRP group disable, 191
    IPv4 VRRP master group following, 190
    IPv6 VRRP group disable, 197
    Monitor Link downlink interface switchover delay, 170
    Monitor Link group creation, 168
    Monitor Link group member interface, 169
    Monitor Link uplink interface switchover threshold, 170
    RRPP ring, 54, 56
    Smart Link group, 146
    Smart Link group configuration (multiple group load sharing), 157
    Smart Link group configuration (single group), 152
    Smart Link group member ports, 149
    Smart Link group protected VLAN, 148
    Smart Link group role preemption mode, 150
    VRRP group router priority, 176

H
hardware
    BFD configuration, 232
health state (RRPP ring), 53
hello
    RRPPDU type, 54
timer (RRPP), 55
high availability
    BFD configuration, 232
    BFD configuration restrictions, 234
    BFD display, 236
    BFD maintain, 236
    BFD protocols and standards, 233
    BFD session and operating modes, 232
    BFD session establishment and termination, 232
    BFD SNMP notification enable, 236
    CFD configuration, 16, 20, 28
    CFD configuration restrictions, 20
    CFD display, 27
    CFD maintain, 27
    CFD protocols and standards, 20
displaying RRPP, 66
    DLD P configuration, 34, 38, 41
    DLD P configuration restrictions, 38
    DLD P hybrid mode, 48
    DLD P manual unidirectional link shutdown, 44
    ERPS configuration, 96
    ERPS configuration (1 ring multi-instance load balancing), 134
    ERPS configuration (1 subring), 120
    Ethernet OAM. See Ethernet OAM
    Ethernet OAM basic configuration, 7
    Ethernet OAM configuration, 7, 14
    Ethernet OAM connection detection timer, 7
    Ethernet OAM display, 13
    Ethernet OAM errored frame event detection, 9
    Ethernet OAM errored frame period event detection, 10
    Ethernet OAM errored frame seconds event detection, 10
    Ethernet OAM errored symbol event detection, 8
    Ethernet OAM functions, 4
    Ethernet OAM link monitoring configuration, 8
    Ethernet OAM maintain, 13
    Ethernet OAM OAMPDUs, 4
    Ethernet OAM port action, 11
    Ethernet OAM protocols and standards, 6
    Ethernet OAM remote loopback, 12
    Ethernet OAM remote loopback configuration restrictions, 12
    Ethernet OAM remote loopback for port (in port view), 13
    Ethernet OAM remote loopback for port (in system view), 12
    Ethernet OAM remote loopback request rejection, 13
evaluation, 1
    EVI IS-IS+Track+BFD collaboration, 276
    fault detection technologies, 2
    IPv4 VRRP configuration, 184, 197
    IPv4 VRRP display, 191
    IPv4 VRRP gratuitous ARP packet periodic send, 189
    IPv4 VRRP group creation, 185
    IPv4 VRRP group disable, 191
    IPv4 VRRP load balancing configuration, 203
    IPv4 VRRP maintain, 191
    IPv4 VRRP master group following, 190
    IPv4 VRRP master group following configuration restrictions, 190
    IPv4 VRRP multiple groups configuration, 200
    IPv4 VRRP operating mode specification, 184
    IPv4 VRRP packet attribute, 187
    IPv4 VRRP router preemptive mode, 186
IPv4 VRRP router priority, 186
IPv4 VRRP router tracking, 186
IPv4 VRRP single group configuration, 197
IPv4 VRRP version specification, 185
IPv4 VRRP virtual IP address assignment, 185
IPv4 VRRPv3 packet sending mode, 188
IPv6 VRRP configuration, 191, 211
IPv6 VRRP display, 197
IPv6 VRRP group creation, 192
IPv6 VRRP group disable, 197
IPv6 VRRP load balancing configuration, 218
IPv6 VRRP maintain, 197
IPv6 VRRP master group following, 196
IPv6 VRRP master group following configuration restrictions, 196
IPv6 VRRP multiple groups configuration, 214
IPv6 VRRP ND periodic packet, 195
IPv6 VRRP operating mode specification, 192
IPv6 VRRP packet attribute, 195
IPv6 VRRP router preemptive mode, 193
IPv6 VRRP router priority, 193
IPv6 VRRP router tracking function, 193
IPv6 VRRP single group configuration, 211
IPv6 VRRP virtual IP address assignment, maintaining RRPP, 66
Monitor Link configuration, 167, 168, 170
Monitor Link configuration restrictions, 168
Monitor Link display, 170
Monitor Link global configuration, 168
Monitor Link group creation, 168
Monitor Link group downlink interface switchover delay, 170
Monitor Link group member interface, 169
Monitor Link group uplink interface switchover threshold, 170
MTBF, 1
MTTR, 1
NQA+Track+static routing collaboration, 238
process placement 1:N process redundancy, 284
process placement configuration, 284, 286
process placement configuration restrictions, 285
process placement display, 288
process placement optimization, 284, 288
process placement policy, 284
process placement policy affinity (location type), 286
process placement policy affinity (location), 286
process placement policy affinity (process), 287
process placement policy affinity (self), 287
process placement policy configuration, 286
protection switchover technologies, 2
redundant Ethernet (Reth) interface configuration, 228, 229, 230
redundant Ethernet (Reth) interface configuration restrictions, 229
removing ERPS ring mode setting, 111
requirements, 1
RRPP configuration, 52, 60, 66
RRPP dual-homed rings configuration, 75
RRPP intersecting rings configuration, 69
RRPP load-balanced intersecting rings configuration, 85
RRPP single ring configuration, 66
RRPP SNMP notification, 66
Smart Link associated device, 151
Smart Link collaboration, 147
Smart Link configuration, 145, 148, 152
Smart Link device, 148
Smart Link display, 152
Smart Link flush message reception, 151
Smart Link flush message send, 150
Smart Link group configuration (multiple group load sharing), 157
Smart Link group configuration (single group), 152
Smart Link group member ports, 149
Smart Link group protected VLAN, 148
Smart Link group role preemption mode, 150
Smart Link maintain, 152
Smart Link+Track collaboration, 151, 161
Smart Link+Track+CFD collaboration, 276
static routing+Track+BFD collaboration, 264
static routing+Track+LLDP collaboration, 273
static routing+Track+NQA collaboration, 260
technologies, 2
Track BFD+VRRP backup master monitor, 254
Track BFD+VRRP master uplink monitor, 256
Track configuration, 237, 238, 250
Track entry display, 250
Track+ ERPS, 249
Track+application module association, 242
Track+BFD association, 239
Track+CFD association, 240
Track+detection module association, 239
Track+EAA, 249
Track+EVI IS-IS, 246
Track+interface management association, 240
Track+LLDP association, 241
Track+MPLS L2VPN, 248
Track+NQA association, 239
Track+policy-based routing, 244
Track+route management association, 241
Track+Smart Link association, 245
Track+static routing association, 243
Track+VPLS, 247
Track+VRRP association, 242
Track+VXLAN, 247
troubleshooting ERPS master node cannot receive SF packets, 144
troubleshooting RRPP master node, 95
troubleshooting VRRP, 226
troubleshooting VRRP error prompt displayed, 226
troubleshooting VRRP fast state flapping, 227
troubleshooting VRRP multiple masters appear in group, 226
VRRP application, 178
VRRP authentication methods, 176
VRRP configuration, 175
VRRP group router priority, 176
VRRP load balancing operating mode, 180
VRRP operating mode, 175
VRRP protocols and standards, 184
VRRP router preemption, 176
VRRP SNMP notification, 191
VRRP standard operating mode, 176
VRRP timers, 177
VRRP tracking, 178
VRRP virtual forwarder (VF), 182
VRRP virtual forwarder (VF) redirect timer, 183
VRRP virtual forwarder (VF) timeout timer, 183
VRRP virtual forwarder (VF) tracking, 184, 188
VRRP virtual MAC address assignment, 180
VRRP+Track+interface management collaboration, 267
VRRP+Track+NQA collaboration, 250
VRRP+Track+route management collaboration, 270

ERPS configuration (1 ring multi-instance load balancing), 134
interface management
VRRP+Track+interface management collaboration, 267
intersecting rings
RRPP intersecting rings configuration, 69
RRPP load balancing, 59
RRPP load-balanced intersecting rings configuration, 85
RRPP network, 57
interval
high availability DLDL advertisement packet send interval, 39
IP addressing
IPv4 VRRP virtual IP address assignment, 185
VRRP configuration, 175
IPv4 VRRP configuration, 175, 184, 197
display, 191
gratuitous ARP packet periodic send, 189
group creation, 185
group disable, 191
load balancing configuration, 203
maintain, 191
master group following, 190
master group following configuration restrictions, 190
multiple groups configuration, 200
operating mode specification, 184
packet attribute configuration, 187
router preemptive mode configuration, 186
router priority configuration, 186
router tracking function configuration, 186
single group configuration, 197
SNMP notification enable, 191
v3 packet sending mode, 188
version specification, 185
virtual forwarder (VF) tracking configuration, 188
virtual IP address assignment, 185
IPv6
BFD protocols and standards, 233
IPv6 VRRP
customization, 175, 191, 211
display, 197
group creation, 192
group disable, 197
load balancing configuration, 218
maintain, 197
master group following, 196

| inactive
| high availability DLDL port state, 35
| initial DLDL port state, 35
| instance
| CFD Ethernet service instance, 21
master group following configuration restrictions, 196
multiple groups configuration, 214
ND periodic packet send, 195
operating mode specification, 192
router preemptive mode, 193
router priority configuration, 193
router tracking function, 193
single group configuration, 211
virtual forwarder tracking (VF) configuration, 194
virtual IP address assignment, 192
IS-IS
EVI IS-IS+Track+BFD collaboration, 276
Track+EVI IS-IS association, 246
L
Layer 2
Ethernet OAM basic configuration, 7
Ethernet OAM configuration, 4, 7, 14
Layer 3
BFD basic configuration, 234
BFD configuration, 232
redundant Ethernet (Reth) interface configuration, 228, 229, 230
link
high availability DLDp DelayDown line failure timer, 39
link
DLDp configuration, 34
DLDp manual unidirectional link shutdown, 44
ERPS configuration, 96
ERPS configuration (1 ring multi-instance load balancing), 134
ERPS configuration (1 subring), 120
Ethernet OAM basic configuration, 7
Ethernet OAM configuration, 4, 7, 14
Ethernet OAM functions, 4
Ethernet OAM link monitoring configuration, 8
Ethernet OAM monitoring, 5
Ethernet OAM port action, 11
high availability DLDp automatic unidirectional link shutdown, 41
high availability DLDp configuration, 38, 41
high availability DLDp hybrid mode, 48
Monitor Link configuration, 167, 168, 170
RRPP link down mechanism, 56
Smart Link backup, 146
Smart Link configuration, 145, 148, 152
Smart Link group configuration (multiple group load sharing), 157
Smart Link group configuration (single group), 152
Smart Link primary/secondary, 146
Smart Link+Track collaboration, 161
link-down RRPPDU type, 54
linktrace (LT)
CFD function, 19
CFD linktrace (LT) configuration, 24
LLDP
static routing+Track+LLDP collaboration, 273
LM
CFD function, 19
CFD LM configuration, 25
load
balancing (RRPP intersecting rings), 59
balancing (RRPP single ring), 58
balancing (RRPP), 55
load balancing
ERPS configuration (1 ring multi-instance load balancing), 134
IPv4 VRRP gratuitous ARP packet periodic send, 189
IPv4 VRRP group creation, 185
IPv4 VRRP group disable, 191
IPv4 VRRP master group following, 190
IPv4 VRRP operating mode specification, 184
IPv4 VRRP packet attribute, 187
IPv4 VRRP router preemptive mode, 186
IPv4 VRRP router priority, 186
IPv4 VRRP router tracking, 186
IPv4 VRRP version specification, 185
IPv4 VRRP virtual IP address assignment, 185
IPv4 VRRPv3 packet sending mode, 188
IPv6 VRRP group creation, 192
IPv6 VRRP group disable, 197
IPv6 VRRP operating mode specification, 192
IPv6 VRRP router preemptive mode, 193
IPv6 VRRP router priority, 193
IPv6 VRRP router tracking function, 193
IPv6 VRRP virtual IP address assignment, 192
RRPP load-balanced intersecting rings configuration, 85
VRRP operating mode, 175, 180
VRRP virtual forwarder (VF), 182
VRRP virtual forwarder (VF) tracking, 188, 194
VRRP virtual MAC address assignment, 180
load sharing
Smart Link, 147
Smart Link group configuration (multiple group load sharing), 157
load-sharing
VRRP application, 179
location
process placement affinity (location type), 286
process placement affinity (location), 286
loop
Smart Link configuration, 145, 148, 152
Smart Link group configuration (multiple group load sharing), 157
Smart Link group configuration (single group), 152
Smart Link+Track collaboration, 161
loopback
CFD function, 19
Ethernet OAM functions, 4
Ethernet OAM remote loopback, 6
loopback (LB)
CFD configuration, 24
M
MAC addressing
VRRP virtual forwarder (VF), 182
VRRP virtual MAC address assignment, 180
maintaining
BFD, 236
CFD, 27
ERPS, 111
Ethernet OAM, 13
high availability DLDP, 40
IPv4 VRRP, 191
IPv6 VRRP, 197
redundant Ethernet (Reth) interface, 229
RRPP, 66
Smart Link, 152
maintenance
association end point. See MEP
association intermediate point. See MIP
CFD 1-way DM configuration, 26
CFD 2-way DM configuration, 26
CFD AIS configuration, 25
CFD continuity check, 23
CFD EAIS configuration, 27
CFD Ethernet service instance configuration, 21
CFD linktrace (LT) configuration, 24
CFD LM configuration, 25
CFD loopback (LB) configuration, 24
CFD maintenance point, 17
CFD MEP configuration, 22
CFD TST configuration, 26
major-fault RRPPDU type, 54
master
RRPP node specification, 63
RRPP node type, 53
VRRP master election, 177
VRRP master/backup application, 178
VRRP multiple masters appear in group, 226
MD5
high availability DLDP authentication, 40
high availability DLDP authentication mode, 36
VRRP authentication, 176
mean time
between failures. Use MTBF
to report. Use MTTR
mechanism
RRPP broadcast storm suppression, 56
RRPP link down, 56
RRPP polling, 55
member port
Smart Link group member ports, 149
memory
process placement configuration, 284, 286
MEP
CFD, 17
CFD 1-way DM configuration, 26
CFD 2-way DM configuration, 26
CFD AIS configuration, 25
CFD continuity check, 23
CFD EAIS configuration, 27
CFD linktrace (LT) configuration, 24
CFD LM configuration, 25
CFD loopback (LB) configuration, 24
CFD MEP configuration, 22
CFD MEP list, 18
CFD TST configuration, 26
message
Smart Link flush, 146
Smart Link flush message reception, 151
Smart Link flush message send, 150
MIP
CFD, 17
CFD MIP auto-generation rule, 22
mode
BFD control packet, 232, 235
BFD control packet active operating, 232
BFD control packet asynchronous operating, 232
BFD control packet demand operating, 232
BFD control packet passive operating, 232
BFD echo packet, 232, 234
BFD multihop detection, 232
BFD single-hop detection, 232
ERPS ring FS mode setting removal, 111
ERPS ring MS mode setting removal, 111
high availability DLDP MD5 authentication, 36
high availability DLDP non-authentication, 36
high availability DLDP plaintext authentication, 36
high availability DLDP port shutdown auto mode, 39
high availability DLDP port shutdown manual mode, 39
IPv4 VRRP router preemptive mode, 186
IPv6 VRRP router preemptive mode, 193
Smart Link group role preemption, 150
Smart Link preemptive, 147
VRRP load balancing operation, 180
VRRP load-balancing operation, 175
VRRP router non-preemptive, 176
VRRP router preemptive, 176
VRRP standard operation, 175, 176
module
EVI IS-IS+Track+BFD collaboration, 276
NQA+Track+static routing collaboration, 238
Smart Link+Track+CFD collaboration, 276
static routing+Track+BFD collaboration, 264
static routing+Track+LLDP collaboration, 273
static routing+Track+NQA collaboration, 260
Track BFD+VRRP backup master monitor, 254
Track BFD+VRRP master uplink monitor, 256
Track configuration, 237, 238, 250
Track+application module association, 242
Track+application module collaboration, 237
Track+detection module association, 239
Track+detection module collaboration, 237
Track+EAA association, 249
Track+ERPS association, 249
Track+EVI IS-IS association, 246
Track+interface management association, 240
Track+LLDP association, 241
Track+MPLS L2VPN association, 248
Track+policy-based routing association, 244
Track+route management association, 241
Track+Smart Link association, 245
Track+static routing association, 243
Track+VPLS association, 247
Track+VRRP association, 242
Track+VXLAN association, 247
VRRP+Track+interface management collaboration, 267
VRRP+Track+NQA collaboration, 250
VRRP+Track+route management collaboration, 270
Monitor Link
configuration, 167, 168, 170
configuration restrictions, 168
display, 170
global configuration, 168
group creation, 168
group downlink interface switchover delay, 170
group member interface configuration, 169
group uplink interface switchover threshold, 170
high availability fault detection technologies, 2
Smart Link collaboration, 147
monitoring
Ethernet OAM link, 5
Ethernet OAM link monitoring configuration, 8
Monitor Link configuration, 167, 168, 170
MPLS L2VPN
Track association, 248
MPU
process placement configuration, 284, 286
MSTP (high availability protection switchover technology), 2
MTBF network availability evaluation, 1
MTTR network availability evaluation, 1
multihop
BFD control packet mode, 235
BFD mode, 232
multiple neighbors detection (DLDP), 38
N
negative (repulse) affinity, 285
neighbor
high availability DLDP multiple neighbors detection, 38
high availability DLDP neighbor state, 35
high availability DLDP single neighbor detection, 36
neighbor discovery (ND)
IPv6 VRRP ND periodic packet send, 195
network
activating RRPP domain, 64
BFD basic configuration, 234
BFD control packet mode configuration, 235
BFD echo packet mode configuration, 234
BFD session and operating modes, 232
BFD session establishment and termination, 232
BFD SNMP notification enable, 236
CFD 1-way DM configuration, 26
CFD 2-way DM configuration, 26
CFD AIS configuration, 25
CFD basic configuration, 21
CFD continuity check, 23
CFD EAIS configuration, 27
CFD enable, 21
CFD Ethernet service instance configuration, 21
CFD function configuration, 23
CFD functions, 18
CFD linktrace (LT) configuration, 24
CFD LM configuration, 25
CFD loopback (LB) configuration, 24
CFD maintenance association, 16
CFD maintenance point, 17
CFD MEP configuration, 22
CFD MEP list, 18
CFD MIP auto-generation rule, 22
CFD TST configuration, 26
configuring RRPP control VLAN, 60
configuring RRPP node, 63
configuring RRPP port, 62
configuring RRPP protected VLAN, 61
configuring RRPP ring, 62
DLDp manual unidirectional link shutdown, 44
ERPS configuration (1 ring multi-instance load balancing), 134
ERPS configuration (1 subring), 120
ERPS ring mode setting removal, 111
ERPS ring structure, 96
Ethernet OAM basic configuration, 7
Ethernet OAM connection detection timer, 7
Ethernet OAM errored frame event detection, 9
Ethernet OAM errored frame period event detection, 10
Ethernet OAM errored frame seconds event detection, 10
Ethernet OAM errored symbol event detection, 8
Ethernet OAM link monitoring configuration, 8
Ethernet OAM port action, 11
Ethernet OAM remote loopback, 12
Ethernet OAM remote loopback for port (in port view), 13
Ethernet OAM remote loopback for port (in system view), 12
Ethernet OAM remote loopback request rejection, 13
EVI IS-IS+Track+BFD collaboration, 276
high availability DLDp multiple neighbors detection, 38
high availability DLDp single neighbor detection, 36
IPv4 VRRP configuration, 184
IPv4 VRRP gratuitous ARP packet periodic send, 189
IPv4 VRRP group creation, 185
IPv4 VRRP group disable, 191
IPv4 VRRP load balancing configuration, 203
IPv4 VRRP master group following, 190
IPv4 VRRP multiple groups configuration, 200
IPv4 VRRP operating mode specification, 184
IPv4 VRRP packet attribute, 187
IPv4 VRRP router preemptive mode, 186
IPv4 VRRP router priority, 186
IPv4 VRRP router tracking, 186
IPv4 VRRP single group configuration, 197
IPv4 VRRP version specification, 185
IPv4 VRRP virtual IP address assignment, 185
IPv4 VRRPv3 packet sending mode, 188
IPv6 VRRP configuration, 191
IPv6 VRRP group creation, 192
IPv6 VRRP group disable, 197
IPv6 VRRP load balancing configuration, 218
IPv6 VRRP master group following, 196
IPv6 VRRP multiple groups configuration, 214
IPv6 VRRP ND periodic packet send, 195
IPv6 VRRP operating mode specification, 192
IPv6 VRRP packet attribute, 195
IPv6 VRRP router preemptive mode, 193
IPv6 VRRP router priority, 193
IPv6 VRRP router tracking function, 193
IPv6 VRRP single group configuration, 211
IPv6 VRRP virtual IP address assignment, 192
Monitor Link group creation, 168
Monitor Link group downlink interface switchover delay, 170
Monitor Link group member interface, 169
Monitor Link group uplink interface switchover threshold, 170
NQA+track+static routing collaboration, 238
process placement optimization, 284, 288
process placement policy, 284
process placement policy affinity (location type), 286
process placement policy affinity (location), 286
process placement policy affinity (self), 287
process placement policy configuration, 286
RRPP assistant-edge type, 53
RRPP edge type, 53
RRPP master type, 53
RRPP transit type, 53
specifying RRPP assistant edge node, 64
specifying RRPP edge node, 64
specifying RRPP master node, 63
specifying RRPP transit node, 63
non.authentication mode (DLDP), 36
notifying
BFD SNMP notification enable, 236
RRPP SNMP notification, 66
VRRP SNMP notification, 191
NQA
static routing+Track+NQA collaboration, 260
Track NQA+Track+static routing collaboration, 238
Track+NQA association, 239
VRRP tracking, 178
VRRP+Track+NQA collaboration, 250
O
OAM
CFD basic configuration, 21
CFD configuration, 16, 20, 28
OAMPDU, 4
operation, administration and maintenance. Use
OAM
optimizing
process placement, 288
process placement optimization, 284
P
packet
BFD control packet mode, 235
BFD echo packet mode, 234
high availability DLDp advertisement packet
send interval, 39
IPv4 VRRP gratuitous ARP packet periodic
send, 189
IPv4 VRRP packet attribute, 187
IPv4 VRRPv3 packet sending mode, 188
IPv6 VRRP master group following, 196
IPv6 VRRP ND periodic packet send, 195
IPv6 VRRP packet attribute, 195
password
high availability DLDp authentication, 40
PBR
Track+policy-based routing association, 244
plaintext
high availability DLDp authentication, 40
high availability DLDp authentication mode, 36
point
CFD maintenance point, 17
CFD MEP, 17
CFD MEP configuration, 22
CFD MIP, 17
policy
process placement affinity (location type), 286
process placement affinity (location), 286
process placement affinity (process), 287
process placement affinity (self), 287
process placement configuration, 286
process placement policy, 284
polling mechanism (RRPP), 55
port
configuring RRPP port, 62
DLDp configuration, 34
DLDp manual unidirectional link shutdown, 44
Ethernet OAM port action, 11
Ethernet OAM remote loopback, 12
Ethernet OAM remote loopback for port (in port
view), 13
Ethernet OAM remote loopback for port (in
system view), 12
Ethernet OAM remote loopback request rejection,
13
high availability DLDp automatic unidirectional
link shutdown, 41
high availability DLDp configuration, 38, 41
high availability DLDp DelayDown timer, 39
high availability DLDp port shutdown mode, 39
high availability DLDp port state, 35
RRPP common, 53
RRPP edge, 53
RRPP primary master, 53
RRPP primary transit, 53
RRPP secondary master, 53
RRPP secondary transit, 53
Smart Link configuration, 145, 148, 152
Smart Link group configuration (multiple group
load sharing), 157
Smart Link group configuration (single group),
152
Smart Link group member ports, 149
Smart Link load sharing, 147
Smart Link primary/secondary, 146
Smart Link+Track collaboration, 161
positive (attract) affinity, 285
preempting
IPv4 VRRP router preemptive mode, 186
IPv6 VRRP router preemptive mode, 193
Smart Link group role preemption mode, 150
Smart Link preemptive mode, 147
VRRP non-preemptive mode, 176
VRRP preemption delay timer, 177
VRRP preemptive mode, 176

primary
RRPP master port, 53
RRPP transit port, 53

priority
IPv4 VRRP router priority, 186
IPv6 VRRP router priority, 193
VRRP group router priority, 176
VRRP virtual forwarder (VF) priority, 182

probe timer (DLDP), 35

procedure
activating RRPP domain, 64
assigning IPv4 VRRP virtual IP address, 185
assigning IPv6 VRRP virtual IP address, 192
associating an ERPS instance port with a track entry, 111
associating Track+application module, 242
associating Track+BFD, 239
associating Track+CFD, 240
associating Track+detection modules, 239
associating Track+EAA, 249
associating Track+ERPS, 249
associating Track+EVI IS-IS, 246
associating Track+interface management, 240
associating Track+LLDP, 241
associating Track+MPLS L2VPN, 248
associating Track+NQA, 239
associating Track+policy-based routing, 244
associating Track+route management, 241
associating Track+Smart Link, 245
associating Track+static routing, 243
associating Track+VPLS, 247
associating Track+VRPP, 242
associating Track+VRRP group, 243
associating Track+VRRP VF, 243
associating Track+VXLAN, 247
configuring associated rings for subrings, 110
configuring BFD basic functions, 234
configuring BFD control packet mode (multihop detection), 235
configuring BFD control packet mode (single-hop detection), 235
configuring BFD echo packet mode, 234
configuring CFD, 20, 28
configuring CFD 1-way DM, 26
configuring CFD 2-way DM, 26
configuring CFD AIS, 25
configuring CFD basic settings, 21
configuring CFD continuity check, 23
configuring CFD EAI, 27
configuring CFD Ethernet service instance, 21
configuring CFD functions, 23
configuring CFD linktrace (LT), 24
configuring CFD LM, 25
configuring CFD loopback (LB), 24
configuring CFD MEP, 22
configuring CFD MIP auto-generation rule, 22
configuring CFD TST, 26
configuring control VLANs, 107
configuring DLDP hybrid mode, 48
configuring ERPS, 112
configuring ERPS (1 ring multi-instance load balancing), 134
configuring ERPS (1 subring), 120
configuring ERPS ring, 105, 105
configuring ERPS ring member port, 105, 106
configuring ERPS ring member port attribute, 106
configuring Ethernet OAM, 7, 14
configuring Ethernet OAM basics, 7
configuring Ethernet OAM connection detection timer, 7
configuring Ethernet OAM errored frame event detection, 9
configuring Ethernet OAM errored frame period event detection, 10
configuring Ethernet OAM errored frame seconds event detection, 10
configuring Ethernet OAM errored symbol event detection, 8
configuring Ethernet OAM link monitoring, 8
configuring Ethernet OAM port action, 11
configuring Ethernet OAM remote loopback, 12
configuring EVI IS-IS+Track+BFD collaboration, 276
configuring high availability DLDP, 38, 41
configuring high availability DLDP authentication, 40
configuring high availability DLDP automatic unidirectional link shutdown, 41
configuring IPv4 VRRP, 184
configuring IPv4 VRRP load balancing, 203
configuring IPv4 VRRP master group following, 190
configuring IPv4 VRRP multiple groups, 200
configuring IPv4 VRRP packet attributes, 187
configuring IPv4 VRRP router preemptive mode, 186
configuring IPv4 VRRP router priority, 186
configuring IPv4 VRRP router tracking function, 186
configuring IPv4 VRRP single group, 197
configuring IPv6 VRRP, 191
configuring IPv6 VRRP load balancing, 218
configuring IPv6 VRRP master group following, 196
configuring IPv6 VRRP multiple groups, 214
configuring IPv6 VRRP packet attribute, 195
configuring IPv6 VRRP router preemptive mode, 193
configuring IPv6 VRRP router priority, 193
configuring IPv6 VRRP router tracking function, 193
configuring Monitor Link, 168, 170
configuring Monitor Link group downlink interface switchover delay, 170
configuring Monitor Link group member interface, 169
configuring Monitor Link group member interface (group view), 169
configuring Monitor Link group member interface (interface view), 169
configuring Monitor Link group uplink interface switchover threshold, 170
configuring node role, 108
configuring one-ring ERPS, 112
configuring process placement, 286
configuring process placement policy, 286
configuring process placement policy affinity (location type), 286
configuring process placement policy affinity (location), 286
configuring process placement policy affinity (process), 287
configuring process placement policy affinity (self), 287
configuring protected VLANs, 107
configuring R-APS packet levels, 109
configuring redundant Ethernet (Reth) interface, 229, 230
configuring RRPP control VLAN, 60
configuring RRPP dual-homed rings, 75
configuring RRPP fail timer, 65
configuring RRPP hello timer, 65
configuring RRPP intersecting rings, 69
configuring RRPP load-balanced intersecting rings, 85
configuring RRPP node, 63
configuring RRPP port, 62
configuring RRPP protected VLAN, 61
configuring RRPP ring, 62
configuring RRPP ring group, 65
configuring RRPP single ring, 66
configuring Smart Link, 148
configuring Smart Link associated device, 151
configuring Smart Link device, 148
configuring Smart Link group (multiple group load sharing), 157
configuring Smart Link group (single group), 152
configuring Smart Link group member port (group view), 149
configuring Smart Link group member port (interface view), 150
configuring Smart Link group protected VLAN, 148
configuring Smart Link group role preemption mode, 150
configuring Smart Link+Track collaboration, 151, 161
configuring Smart Link+Track+CFD collaboration, 276
configuring static routing+Track+BFD collaboration, 264
configuring static routing+Track+LLDP collaboration, 273
configuring static routing+Track+NQA collaboration, 260
configuring Track, 238
configuring Track BFD+VRRP backup master monitor, 254
configuring Track BFD+VRRP master uplink monitor, 256
configuring VRRP virtual forwarder (VF) tracking, 188
configuring VRRP virtual forwarder tracking (VF), 194
configuring VRRP+Track+interface management collaboration, 267
configuring VRRP+Track+NQA collaboration, 250
configuring VRRP+Track+route management collaboration, 270
creating IPv4 VRRP group, 185
creating IPv6 VRRP group, 192
creating Monitor Link group, 168
creating RRPP domain, 60
disabling IPv4 VRRP group, 191
disabling IPv6 VRRP group, 197
displaying BFD, 236
displaying CFD, 27
displaying ERPS, 111
displaying Ethernet OAM, 13
displaying high availability DLDP, 40
displaying IPv4 VRRP, 191
enabling BFD SNMP notifications, 236
enabling CFD, 21
enabling ERPS for instance, 108
enabling ERPS globally, 104
enabling Ethernet OAM remote loopback for port (in port view), 13
enabling Ethernet OAM remote loopback for port (in system view), 12
enabling flush packet transparent transmission, 105
enabling high availability DLDp, 39
enabling IPv4 VRRP gratuitous ARP packet periodic send, 189
enabling IPv6 VRRP ND periodic packet send, 195
enabling Monitor Link globally, 168
enabling R-APS packets to carry the ring ID in the destination MAC address, 105
enabling RRPP SNMP notification, 66
enabling Smart Link flush message receiving, 151
enabling Smart Link flush message send, 150
enabling VRRP SNMP notification, 191
maintaining BFD, 236
maintaining CFD, 27
maintaining ERPS, 111
maintaining Ethernet OAM, 13
maintaining high availability DLDp, 40
maintaining IPv4 VRRP, 191
maintaining IPv6 VRRP, 197
maintaining redundant Ethernet (Reth) interface, 229
maintaining Smart Link, 152
optimizing process placement, 288
rejecting Ethernet OAM remote loopback request, 13
removing ERPS ring mode setting, 111
setting ERPS timers, 109
setting high availability DLDp advertisement packet send interval, 39
setting high availability DLDp DelayDown timer, 39
setting high availability DLDp port shutdown mode, 39
setting IPv4 VRRPv3 packet sending mode, 188
setting the FS mode, 110
setting the MS mode, 110
setting the non-revertive mode, 109
shutting down DLDp unidirectional link manually, 44
specifying IPv4 VRRP operating mode, 184
specifying IPv4 VRRP version, 185
specifying IPv6 VRRP operating mode, 192
specifying RRPP assistant edge node, 64
specifying RRPP edge node, 64
specifying RRPP master node, 63
specifying RRPP transit node, 63
troubleshooting ERPS master node cannot receive SF packets, 144
troubleshooting RRPP master node, 95
troubleshooting VRRP error prompt displayed, 226
troubleshooting VRRP fast state flapping, 227
troubleshooting VRRP multiple masters appear in group, 226
process placement
1:N process redundancy, 284
configuration, 284, 286
configuration restrictions, 285
display, 288
optimization, 284, 288
policy, 284
policy affinity configuration (location type), 286
policy affinity configuration (location), 286
policy affinity configuration (process), 287
policy affinity configuration (self), 287
policy configuration, 286
protected VLAN
RRPP configuration, 61
Smart Link, 146
Smart Link group protected VLAN, 148
Smart Link load sharing, 147
protected VLAN (RRPP), 53
protection switching (PS)
ERPS configuration, 96
ERPS configuration (1 ring multi-instance load balancing), 134
ERPS configuration (1 subring), 120
protection switchover (high availability technology), 2
protocols and standards
BFD, 233
CFD, 20
Ethernet OAM, 6
RRPP, 59
RRPP configuration, 52, 60, 66
VRRP, 184

R

Rapid Ring Protection Protocol. See RRPP
R-APS packet levels
configuration, 109
receive control VLAN
Smart Link, 146
receiving
Smart Link flush message reception, 151
Smart Link receive control VLAN, 146
recovering RRPP ring, 56
recover probe timer (DLDP), 35
redundancy
process placement 1:N process redundancy, 284
redundant Ethernet (Reth) interface
application scenario, 228
configuration, 228, 229, 230
configuration restrictions, 229
display, 229
maintain, 229
operating mechanism, 228
rejecting
Ethernet OAM remote loopback request, 13
remote
Ethernet OAM fault detection, 6
Ethernet OAM remote loopback, 6, 12
Ethernet OAM remote loopback for port (in port view), 13
Ethernet OAM remote loopback for port (in system view), 12
Ethernet OAM remote loopback request rejection, 13
removing
ERPS ring mode setting, 111
requirements (high availability), 1
restrictions
BFD configuration, 234
CFD configuration, 20
DLDP configuration, 38
Ethernet OAM remote loopback configuration, 12
IPv4 VRRP master group following configuration, 190
IPv6 VRRP master group following configuration, 196
Monitor Link configuration, 168
process placement configuration, 285
redundant Ethernet (Reth) interface configuration, 229

ring
configuring (RRPP), 62
configuring RRPP group, 65
disconnect state (RRPP), 53
Ethernet ring protection switching. Use ERPS
health state (RRPP), 53
recovery (RRPP), 56
RRPP group, 54, 56

role
Smart Link group role preemption mode, 150
route management
VRRP+Track+route management collaboration, 270

router
IPv4 VRRP router preemptive mode, 186
IPv4 VRRP router priority, 186
IPv4 VRRP router tracking, 186
IPv6 VRRP router preemptive mode, 193
IPv6 VRRP router priority, 193
IPv6 VRRP router tracking function, 193
Virtual Router Redundancy Protocol. Use VRRP
VRRP group priority, 176
VRRP master election, 177
VRRP preemption modes, 176

routing
DLDP configuration, 34
DLDP manual unidirectional link shutdown, 44
Ethernet OAM port action, 11
Ethernet OAM remote loopback, 12
Ethernet OAM remote loopback for port (in port view), 13
Ethernet OAM remote loopback for port (in system view), 12
Ethernet OAM remote loopback request rejection, 13
high availability DLDP automatic unidirectional link shutdown, 41
high availability DLDP configuration, 38, 41
Monitor Link configuration, 167, 168, 170
static routing+Track+BFD collaboration, 264
static routing+Track+LLDP collaboration, 273
static routing+Track+NQA collaboration, 260
Track+policy-based routing association, 244
VRRP configuration, 175

RRPP
activating domain, 64
assistant-edge node type, 53
basic concepts, 52
broadcast storm suppression, 56
common port, 53
common-flush-FDB RRPPDU, 54
complete-flush-FDB RRPPDU, 54
configuration, 52, 60, 66
configuring control VLAN, 60
configuring fail timer, 65
configuring hello timer, 65
configuring node, 63
configuring port, 62
configuring protected VLAN, 61
configuring ring, 62
configuring ring group, 65
control VLAN, 53
creating domain, 60
displaying, 66
domain, 52
dual-homed rings configuration, 75
dual-homed rings networking, 58
edge node type, 53
edge port, 53
edge-hello RRPPDU, 54
fail timer, 55
hello RRPPDU, 54
hello timer, 55
how it works, 55
intersecting rings configuration, 69
intersecting rings load balancing, 59
intersecting rings networking, 57
link down mechanism, 56
link-down RRPPDU, 54
load balancing, 55
load-balanced intersecting rings configuration, 85
maintaining, 66
major-fault RRPPDU, 54
master node type, 53
networking, 56
node types, 53
polling mechanism, 55
primary master port, 53
primary transit port, 53
protected VLAN, 53
protocols and standards, 59
ring group, 54, 56
ring recovery, 56
ring topology, 53
secondary master port, 53
secondary transit port, 53
single ring configuration, 66
single ring load balancing, 58
single ring networking, 56
specifying assistant edge node, 64
specifying edge node, 64
specifying master node, 63
specifying transit node, 63
tangent rings networking, 57
transit node type, 53
troubleshoot master node, 95
RRPP (high availability protection switchover technology), 2
RRPPDU, 53
common-flush-FDB type, 54
complete-flush-FDB type, 54
edge-hello type, 54
hello type, 54
link-down type, 54
major-fault type, 54
rule
CFD MIP auto-generation, 22
CFD MIP default rule, 17
CFD MIP explicit rule, 17
S
secondary
RRPP master port, 53
RRPP transit port, 53
security
high availability DLDLP authentication, 40
high availability DLDLP authentication modes, 36
VRRP MD5 authentication, 176
VRRP simple authentication, 176
self affinity (process placement), 287
sending
Smart Link flush message send, 150
session
BFD control packet active operating mode, 232
BFD control packet asynchronous operating mode, 232
BFD control packet demand operating mode, 232
BFD control packet mode, 232
BFD control packet passive operating mode, 232
BFD echo packet mode, 232
BFD session establishment and termination, 232
setting
ERPS FS mode, 110
ERPS MS mode, 110
ERPS non-revertive mode, 109
ERPS timers, 109
high availability DLDLP advertisement packet send interval, 39
high availability DLDLP DelayDown timer, 39
high availability DLDLP port shutdown mode, 39
IPv4 VRRIPv3 packet sending mode, 188
shutting down
  DLDL unidirectional link manually, 44
  high availability DLDL automatic unidirectional link shutdown, 41
  high availability DLDL port shutdown mode, 39
simple authentication
  VRRP, 176
single
  RRPP ring network, 56
  RRPP ring network load balancing, 58
single-hop
  BFD control packet mode, 235
  BFD mode, 232
Skew-Time (VRRP), 177
Smart Link
  associated device configuration, 151
  collaboration, 147
  configuration, 145, 148, 152
  device configuration, 148
  display, 152
  flush message reception enable, 151
  flush message send enable, 150
  group configuration (multiple group load sharing), 157
  group configuration (single group), 152
  group member port configuration, 149
  group protected VLAN configuration, 148
  group role preemption mode configuration, 150
  how it works, 146
  maintain, 152
  Monitor Link collaboration, 147
  Smart Link+Track+CFD collaboration, 276
  terminology, 146
  Track collaboration, 147, 161
  Track collaboration configuration, 151
  Track+Smart Link association, 245
Smart Link (high availability protection switchover technology), 2
SNMP
  BFD SNMP notification enable, 236
  RRPP SNMP notification, 66
  VRRP SNMP notification, 191
specifying
  IPv4 VRRP operating mode, 184
  IPv4 VRRP version, 185
  IPv6 VRRP operating mode, 192
  RRPP assistant edge node, 64
  RRPP edge node, 64
  RRPP master node, 63
  RRPP transit node, 63
SRPT (RRPP broadcast storm suppression mechanism), 56
standard
  VRRP operating mode, 175, 176
standby
  switchover (high availability technologies), 2
state
  high availability DLDL neighbor state, 35
  high availability DLDL port state, 35
  RRPP ring disconnect state, 53
  RRPP ring health state, 53
static routing
  NQA+Track+static routing collaboration, 238
  static routing+Track+BFD collaboration, 264
  static routing+Track+LLDP collaboration, 273
  static routing+Track+NQA collaboration, 260
  Track+static routing association, 243
structure
  ERPS ring structure, 96
subnetting
  IPv4 VRRP configuration, 184, 197
  IPv4 VRRP load balancing configuration, 203
  IPv4 VRRP multiple groups configuration, 200
  IPv4 VRRP single group configuration, 197
  IPv6 VRRP configuration, 191, 211
  IPv6 VRRP load balancing configuration, 218
  IPv6 VRRP multiple groups configuration, 214
  IPv6 VRRP single group configuration, 211
  VRRP configuration, 175
switchover
t  protection switchover technologies (high availability), 2
termination
  Monitor Link group downlink interface switchover delay, 170
  Monitor Link group uplink interface switchover threshold, 170
T
tangent rings (RRPP network), 57
terminating
  BFD session, 232
testing
  CFD TST configuration, 26
time
  MTBF, 1
  MTTR, 1
timer
c  configuring RRPP fail, 65
configuring RRPP hello, 65
Ethernet OAM connection detection, 7
high availability DLD advertisement, 35
high availability DLD DelayDown, 35, 39
high availability DLD echo, 35
high availability DLD enhanced, 35
high availability DLD entry, 35
high availability DLD probe, 35
high availability DLD recoverProbe, 35
RRPP fail, 55
RRPP hello, 55
VRRP advertisement interval, 177
VRRP preemption delay timer, 177
VRRP skew-time, 177
VRRP virtual forwarder (VF) redirect, 183
VRRP virtual forwarder (VF) timeout, 183
topology
configuring RRPP port, 63
configuring RRPP ring, 62
ERPS configuration, 96
ERPS configuration (1 ring multi-instance load balancing), 134
ERPS configuration (1 subring), 120
ERPS ring mode setting removal, 111, 111
RRPP configuration, 52, 60, 66
RRPP domain, 52
RRPP dual-homed rings, 58
RRPP dual-homed rings configuration, 75
RRPP intersecting rings, 57
RRPP intersecting rings configuration, 69
RRPP load-balanced intersecting rings configuration, 85
RRPP networking, 56
RRPP ring group, 56
RRPP single ring, 56
RRPP single ring configuration, 66
RRPP tangent rings, 57
Smart Link change, 147
Smart Link configuration, 145, 148, 152
Smart Link group configuration (multiple group load sharing), 157
Smart Link group configuration (single group), 152
Smart Link+Track collaboration, 161
Track
application module association, 242
application module collaboration, 237
BFD association, 239
BFD+VRRP backup master monitor configuration, 254
BFD+VRRP master uplink monitor configuration, 256
CFD association, 240
configuration, 237, 238, 250
detection module association, 239
detection module collaboration, 237
EAA association, 249
entry display, 250
ERPS association, 249
EVI IS-IS association, 246
EVI IS-IS+Track+BFD collaboration configuration, 276
high availability fault detection technologies, 2
interface management association, 240
IPv4 VRRP router tracking, 186
IPv6 VRRP router tracking function, 193
LLDP association, 241
MPLS L2VPN association, 248
NQA association, 239
NQA+Track+static routing collaboration, 238
policy-based routing association, 244
route management association, 241
Smart Link association, 245
Smart Link collaboration, 147, 151, 161
Smart Link+Track+CFD collaboration configuration, 276
static routing association, 243
static routing+Track+BFD collaboration configuration, 264
static routing+Track+LLDP collaboration configuration, 273
static routing+Track+NQA collaboration configuration, 260
VPLS association, 247
VRRP association, 242
VRRP group association, 243
VRRP VF association, 243
VRRP+Track+interface management collaboration configuration, 267
VRRP+Track+NQA collaboration configuration, 250
VRRP+Track+route management collaboration configuration, 270
VXLAN association, 247
tracking
VRRP, 178
VRRP virtual forwarder (VF) tracking, 184
traffic
redundant Ethernet (Reth) interface configuration, 228, 229, 230
RRPP load balancing, 55
Smart Link load sharing, 147
transit node
RRPP type, 53
specifying RRPP, 63
transmit control VLAN
Smart Link, 146
transmitting
Smart Link transmit control VLAN, 146
trapping
BFD SNMP notification enable, 236
VRRP SNMP notification, 191
troubleshooting
ERPS master node cannot receive SF packets, 144
RRPP master node, 95
VRRP, 226
VRRP error prompt displayed, 226
VRRP fast state flapping, 227
VRRP multiple masters appear in group, 226
TST
CFD function, 20
CFD TST configuration, 26
U
unconfirmed DLDP neighbor state, 35
unidirectional
DLDP manual unidirectional link shutdown, 44
high availability DLDP automatic unidirectional link shutdown, 41
high availability DLDP port state, 35
updating
Smart Link flush update, 147
Smart Link uplink traffic triggered MAC address learning, 147
uplink
Monitor Link group uplink interface switchover threshold, 170
Smart Link uplink traffic triggered MAC address learning, 147
Track BFD+VRRP master uplink monitor, 256
V
version
IPv4 VRRP specification, 185
virtual
IPv4 VRRP virtual IP address assignment, 185
IPv6 VRRP virtual IP address assignment, 192
Virtual Router Redundancy Protocol. Use VRRP
VRRP virtual forwarder (VF), 182
VRRP virtual forwarder tracking (VF), 194
VRRP virtual MAC address assignment, 180
VLAN
CFD basic configuration, 21
CFD configuration, 16, 20, 28
CFD Ethernet service instance configuration, 21
CFD function configuration, 23
CFD functions, 18
CFD maintenance association, 16
CFD maintenance point, 17
CFD MIP auto-generation rule, 22
configuring RRPP control VLAN, 60
configuring RRPP port, 62
configuring RRPP protected VLAN, 61
control (RRPP), 53
protected (RRPP), 53
RRPP domain, 52
RRPP load balancing, 55
Smart Link configuration, 145, 148, 152
Smart Link group configuration (multiple group load sharing), 157
Smart Link group configuration (single group), 152
Smart Link group protected VLAN, 148
Smart Link load sharing, 147
Smart Link protected VLAN, 146
Smart Link receive control VLAN, 146
Smart Link transmit control VLAN, 146
Smart Link+Track collaboration, 161
VPLS
Track+VPLS association, 247
VRRP
application, 178
authentication methods, 176
configuration, 175
group router priority, 176
high availability protection switchover technologies, 2
IPv4 gratuitous ARP packet periodic send, 189
IPv4 master group following, 190
IPv4 VRRPv3 packet sending mode, 188
IPv6 group disable, 197
IPv6 master group following, 196
IPv6 ND periodic packet send, 195
IPv6 packet attribute, 195
load-sharing application, 179
master election, 177
master/backup application, 178
operating mode, 175
operating mode (load balancing), 180
operating mode (standard), 176
protocols and standards, 184
router preemption, 176

Timers, 177

Track BFD+VRRP backup master monitor, 254

Track BFD+VRRP master uplink monitor, 256

Track+VRRP association, 242

Track+VRRP group association, 243

Track+VRRP VF association, 243

Tracking, 178

Troubleshoot, 226

Troubleshoot error prompt displayed, 226

Troubleshoot fast state flapping, 227

Troubleshoot multiple masters appear in group, 226

Virtual forwarder (VF), 182

Virtual forwarder (VF) backup, 182

Virtual forwarder (VF) creation, 182

Virtual forwarder (VF) redirect timer, 183

Virtual forwarder (VF) timeout timer, 183

Virtual forwarder (VF) tracking, 184

Virtual forwarder (VF) weight/priority, 182

Virtual forwarder tracking (VF) configuration, 194

Virtual MAC address assignment, 180

VRRP+Track+Interface management collaboration, 267

VRRP+Track+NQA collaboration, 250

VRRP+Track+route management collaboration, 270

W

Weight

VRRP virtual forwarder (VF), 182