HP 5120 SI Switch Series

High Availability

Configuration Guide

Part number: 5998-1819
Software version: Release 1505
Document version: 6W102-20121111

Legal and notice information

The information contained herein is subject to change without notice.

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

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

Contents

High availability overview 1
Availability requirements 1
Availability evaluation 1
High availability technologies 2
Fault detection technologies 2
Protection switchover technologies 3

Ethernet OAM configuration 4
Ethernet OAM overview 4
Background 4
Major functions of Ethernet OAM 4
Ethernet OAMPDUs 4
How Ethernet OAM works 6
Protocols and Standards 8
Ethernet OAM configuration task list 8
Configuring basic Ethernet OAM functions 8
Configuring the Ethernet OAM connection detection timers 9
Configuring link monitoring 9
Configuring errored symbol event detection 10
Configuring errored frame event detection 10
Configuring errored frame period event detection 10
Configuring errored frame seconds event detection 11
Configuring OAM remote loopback 11
Displaying and maintaining Ethernet OAM configuration 12
Ethernet OAM configuration example 12

CFD configuration 15
Overview 15
Basic concepts in CFD 15
CFD functions 17
Protocols and standards 19
CFD configuration task list 19
Configuring basic CFD settings 20
Enabling CFD 20
Configuring the CFD protocol version 20
Configuring service instances 21
Configuring MEPs 21
Configuring MIP generation rules 22
Configuring CFD functions 23
Configuration prerequisites 23
Configuring CC on MEPs 23
Configuring LB on MEPs 24
Configuring LT on MEPs 24
Configuring AIS 25
Configuring LM 25
Configuring one-way DM 26
Configuring two-way DM 26
Configuring TST 26
Displaying and maintaining CFD 27
CFD configuration example 28

DLDP configuration 34
Overview 34
Background 34
How DLDP works 35
DLDP configuration task list 41
Enabling DLDP 41
Setting DLDP mode 42
Setting the interval for sending advertisement packets 42
Setting the DelayDown timer 43
Setting the port shutdown mode 43
Configuring DLDP authentication 44
Resetting DLDP state 44
Displaying and maintaining DLDP 45
DLDP configuration examples 45
Automatically shutting down unidirectional links 45
Manually shutting down unidirectional links 49
Troubleshooting DLDP 52

Smart Link configuration 53
Smart Link overview 53
Background 53
Terminology 54
How Smart Link works 55
Smart Link collaboration mechanisms 56
Smart Link configuration task list 56
Configuring a smart link device 56
Configuration prerequisites 56
Configuring protected VLANs for a smart link group 57
Configuring member ports for a smart link group 57
Configuring role preemption for a smart link group 57
Enabling the sending of flush messages 58
Configuring an associated device 58
Configuration prerequisites 58
Enabling the receiving of flush messages 59
Displaying and maintaining Smart Link 59
Smart Link configuration examples 59
Single smart link group configuration example 59
Multiple smart link groups load sharing configuration example 64

Monitor Link configuration 69
Overview 69
Terminology 69
How Monitor Link works 70
Configuring Monitor Link 70
Configuration prerequisites 70
Creating a monitor link group 70
Configuring monitor link group member ports 70
Displaying and maintaining Monitor Link 71
Monitor Link configuration example 71

Support and other resources 75
Contacting HP 75
Subscription service 75
Related information 75
Documents 75
Websites 75

Conventions 76
Index 78

High availability overview

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

The following are the effective ways to improve availability:

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

Availability requirements

Availability requirements fall into three levels based on purpose and implementation, as shown in Table 1.

Table 1 Availability requirements

Level	Requirement	Solution
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 by failures	Device and link redundancy and switchover
3	Enable the system to recover as fast as possible	Fault detection, diagnosis, isolation, and recovery technologies

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

Availability evaluation

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

MTBF

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

MTTR

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

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

High availability technologies

As previously mentioned, increasing MTBF or decreasing MTTR can enhance the availability of a network. The high availability technologies described in this section meet the 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. CFD, DLDP, and Ethernet OAM are data link layer fault detection technologies; NQA is used for diagnosis and evaluation of network quality; Monitor Link work along with other high availability technologies to detect faults through a collaboration mechanism. For more information about these technologies, see Table 2.

Table 2 Fault detection technologies

Technology	Introduction	Reference
CFD	Connectivity Fault Detection (CFD), which conforms to IEEE 802.1ag Connectivity Fault Management (CFM) and ITU-T Y.1731, is an end-to-end per-VLAN link layer Operations, Administration and Maintenance (OAM) mechanism used for link connectivity detection, fault verification, and fault location.	CFD configuration in the *High Availability Configuration Guide*
DLDP	The Device link detection protocol (DLDP) deals with unidirectional links that may occur in a network. On detecting a unidirectional link, DLDP, as configured, can shut down the related port automatically or prompt users to take actions to avoid network problems.	DLDP configuration in the *High Availability Configuration Guide*
Ethernet OAM	As a tool monitoring Layer 2 link status, Ethernet OAM is mainly used to address common link-related issues on the "last mile". You can monitor the status of the point-to-point link between two directly connected devices by enabling Ethernet OAM on them.	Ethernet OAM configuration in the *High Availability Configuration Guide*
NQA	Network Quality Analyzer (NQA) analyzes network performance, services and service quality through sending test packets, and provides you with network performance and service quality parameters such as jitter, TCP connection delay, FTP connection delay and file transfer rate.	NQA configuration in the *Network Management and Monitoring Configuration Guide*
Monitor Link	Monitor link is a port collaboration function. It is usually used in conjunction with Layer 2 topology protocols. The idea is to monitor the states of uplink ports and adapt the up/down state of downlink ports to the up/down state of uplink ports, triggering link switchover on the downstream device in time.	Monitor link configuration in the *High Availability Configuration Guide*

Protection switchover technologies

Protection switchover technologies aim at recovering network faults. They back up hardware, link, routing, and service information for switchover in case of network faults to ensure continuity of network services. For more information about protection switchover technologies, see Table 3.

Table 3 Protection switchover technologies

Technology	Introduction	Reference
Ethernet Link Aggregation	Ethernet link aggregation, most often simply called "link aggregation", aggregates multiple physical Ethernet links into one logical link to increase link bandwidth beyond the limits of any one single link. This logical link is called an aggregate link. It allows for link redundancy because the member physical links can dynamically back up one another.	Ethernet link aggregation configuration in the *Layer 2—LAN Switching Configuration Guide*
Smart Link	Smart Link is a feature developed to address the slow convergence issue with STP. It provides link redundancy as well as fast convergence in a dual uplink network, allowing the backup link to take over quickly when the primary link fails.	Smart link configuration in the *High Availability Configuration Guide*
MSTP	As a Layer 2 management protocol, the Multiple Spanning Tree Protocol (MSTP) eliminates Layer 2 loops by selectively blocking redundant links in a network, and in the mean time, allows for link redundancy.	MSTP configuration in the *Layer 2—LAN Switching Configuration Guide*

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

Ethernet OAM configuration

This chapter includes these sections:

- Ethernet OAM overview
- Ethernet OAM configuration task list
- Configuring basic Ethernet OAM functions
- Configuring the Ethernet OAM connection detection timers
- Configuring OAM remote loopback
- Displaying and maintaining Ethernet OAM configuration
- Ethernet OAM configuration example

Ethernet OAM overview

Background

Ethernet, because of its ease of use and low price, has become the major underlying technology for local area networks (LANs). With the emergence of Gigabit Ethernet and 10-Gigabit Ethernet, Ethernet is gaining popularity in metropolitan area networks (MANs) and wide area networks (WANs) as well, increasing the need for an effective management and maintenance mechanism for Ethernet. This makes it urgent to implement Operation, Administration and Maintenance (OAM) on Ethernet networks.

As a tool monitoring Layer 2 link status, Ethernet OAM mainly addresses common link-related issues on the "last mile." When you enable Ethernet OAM on two devices connected by a point-to-point link, you can monitor the status of the link.

Major functions of Ethernet OAM

Ethernet OAM is an effective tool for management and maintenance of Ethernet networks, helping to ensure network stability. It includes the following major functions:

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

Ethernet OAMPDUs

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

Figure 1 Formats of different types of Ethernet OAMPDUs

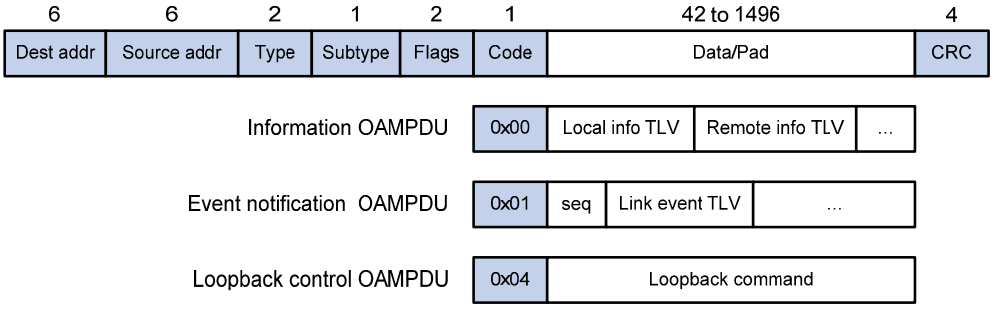


Table 4 Description of the fields in an OAMPDU

Field	Description
Dest addr	Destination MAC address of the Ethernet OAMPDU It is a slow protocol multicast address 0180c2000002. As slow protocol packet cannot be forwarded by bridges, Ethernet OAMPDUs cannot be forwarded.
Source addr	Source MAC address of the Ethernet OAMPDU It is the bridge MAC address of the sending side and is a unicast MAC address.
Type	Type of the encapsulated protocol in the Ethernet OAMPDU The value is 0x8809.
Subtype	The specific protocol being encapsulated in the Ethernet OAMPDU The value is 0x03.
Flags	Status information of an Ethernet OAM entity
Code	Type of the Ethernet OAMPDU

NOTE:

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

Table 5 Functions of different types of OAMPDUs

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

How Ethernet OAM works

This section describes the working procedures of Ethernet OAM.

Ethernet OAM connection establishment

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

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

As for Ethernet OAM connection establishment, a device can operate in active Ethernet OAM mode or passive Ethernet OAM mode.

Table 6 Active and passive Ethernet OAM modes

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

NOTE:

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

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

Link monitoring

Error detection in an Ethernet is difficult, especially when the physical connection in the network is not disconnected but network performance is degrading gradually. Link monitoring is used to detect and indicate link faults in various environments. Ethernet OAM implements link monitoring through the

exchange of Event Notification OAMPDUs. When detecting a link error event listed in Table 7, the local OAM entity sends an Event Notification OAMPDU to notify the remote OAM entity. With the log information, network administrators can keep track of network status in time.

Table 7 Ethernet OAM link error events

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

NOTE:

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

Remote fault detection

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

Table 8 Critical link events

Type	Description	OAMPDU transmission frequencies
Link Fault	Peer link signal is lost.	Once per second
Dying Gasp	An unexpected fault, such as power failure, occurred.	Non-stop
Critical Event	An undetermined critical event happened.	Non-stop

NOTE:

- 5120 SI Switch Series is able to receive information OAMPDUs carrying the critical link events listed in Table 8.
- Only the Gigabit optical ports are able send information OAMPDUs carrying Link Fault events.
- 5120 SI Switch Series is able to send information OAMPDUs carrying Dying Gasp events when the device is rebooted or relevant ports are manually shut down. Physical IRF ports, however, are unable to send this type of OAMPDUs. For more information about physical IRF ports, see the *IRF Configuration Guide*.
- 5120 SI Switch Series is unable to send information OAMPDUs carrying Critical Events.

Remote loopback

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

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

Protocols and Standards

IEEE 802.3h, *Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*

Ethernet OAM configuration task list

Complete the following tasks to configure Ethernet OAM:

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

Configuring basic Ethernet OAM functions

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

Follow these steps to configure basic Ethernet OAM functions:

To do…	Use the command…	Remarks
Enter system view	**System-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the Ethernet OAM mode	**oam mode** { **active** | **passive** }	Optional The default is active Ethernet OAM mode.
Enable Ethernet OAM on the current port	**oam enable**	Required Ethernet OAM is disabled by default.

NOTE:

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

Configuring the Ethernet OAM connection detection timers

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

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

Follow these steps to configure the Ethernet OAM connection detection timers:

To do…	Use the command…	Remarks
Enter system view	**System-view**	—
Configure the Ethernet OAM handshake packet transmission interval	**oam timer hello** *interval*	Optional 1000 millisecond by default
Configure the Ethernet OAM connection timeout timer	**oam timer keepalive** *interval*	Optional 5000 milliseconds by default

CAUTION:

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

Configuring link monitoring

NOTE:

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

Configuring errored symbol event detection

An errored symbol event occurs when the number of detected symbol errors over a specific detection interval exceeds the configured threshold.

Follow these steps to configure errored symbol event detection:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the errored symbol event detection interval	**oam errored-symbol period** *period-value*	Optional 1 second by default
Configure the errored symbol event triggering threshold	**oam errored-symbol threshold** *threshold-value*	Optional 1 by default

Configuring errored frame event detection

An errored frame event occurs when the number of detected error frames over a specific interval exceeds the configured threshold.

Follow these steps to configure errored frame event detection:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the errored frame event detection interval	**oam errored-frame period** *period-value*	Optional 1 second by default
Configure the errored frame event triggering threshold	**oam errored-frame threshold** *threshold-value*	Optional 1 by default

Configuring errored frame period event detection

An errored frame period event occurs if the number of frame errors in specific number of received frames exceeds the configured threshold.

Follow these steps to configure errored frame period event detection:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the errored frame period event detection period	**oam errored-frame-period period** *period-value*	Optional 1000 milliseconds by default

To do…	Use the command…	Remarks
Configure the errored frame period event triggering threshold	**oam errored-frame-period threshold** *threshold-value*	Optional 1 by default

Configuring errored frame seconds event detection

An errored frame seconds event occurs when the number of error frame seconds detected on a port over a detection interval exceeds the error threshold.

Follow these steps to configure errored frame seconds event detection:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the errored frame seconds event detection interval	**oam errored-frame-seconds period** *period-value*	Optional 60 second by default
Configure the errored frame seconds event triggering threshold	**oam errored-frame-seconds threshold** *threshold-value*	Optional 1 by default

CAUTION:

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

Configuring OAM remote loopback

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

Follow these steps to enable Ethernet OAM remote loopback in interface view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Layer 2 Ethernet port view	**interface** *interface-type interface-number*	—
Enable Ethernet OAM remote loopback on the port	**oam loopback**	Required Disabled by default.

NOTE:

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

NOTE:

- Ethernet OAM remote loopback is available only after the Ethernet OAM connection is established and can be performed only by the Ethernet OAM entities operating in active Ethernet OAM mode.
- Remote loopback is available only on full-duplex links that support remote loopback at both ends.
- Ethernet OAM remote loopback needs the support of the peer hardware.
- Enabling Ethernet OAM remote loopback interrupts data communications. After Ethernet OAM remote loopback is disabled, all the ports involved will shut down and then come up. Ethernet OAM remote loopback is disabled when you execute the **undo oam enable** command to disable Ethernet OAM, when you execute the **undo oam loopback** command to disable Ethernet OAM remote loopback, or when the Ethernet OAM connection times out.
- Ethernet OAM remote loopback is only applicable to individual links. It is not applicable to link aggregation member ports. In addition, do not assign ports where Ethernet OAM remote loopback is being performed to link aggregation groups. For more information about link aggregation groups, see the *Layer 2—LAN Switching Configuration Guide*.
- Enabling internal loopback test on a port in remote loopback test can terminate the remote loopback test. For more information about loopback test, see the *Layer 2—LAN Switching Configuration Guide*.

Displaying and maintaining Ethernet OAM configuration

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

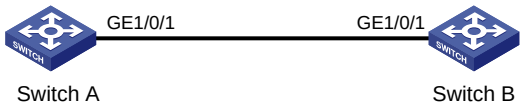
Ethernet OAM configuration example

Network requirements

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

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

Figure 2 Network diagram for Ethernet OAM configuration



Configuration procedure

1. Configure Switch A

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

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

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

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

2. Configure Switch B

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

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

3. Verify the configuration

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

Display the Ethernet OAM configuration on Switch A.

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

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

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

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

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

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

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

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

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

```
[SwitchB] display oam link-event remote
Port :GigabitEthernet1/0/1
Link Status :Up
OAMRemoteErrFrameEvent : (ms = milliseconds)
------------------------------------------------------------------------
Event Time Stamp          : 5789        Errored FrameWindow   : 10(100ms)
Errored Frame Threshold   : 1           Errored Frame         : 3
Error Running Total       : 35          Event Running Total   : 17
```

The output indicates that 35 errors occurred since Ethernet OAM was enabled on Switch A, 17 of which are caused by error frames. The link is instable.

CFD configuration

This chapter includes these sections:

- Overview
- CFD configuration task list
- Displaying and maintaining CFD
- CFD configuration example

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 Operations, Administration and Maintenance (OAM) mechanism used for link connectivity detection, fault verification, and fault location.

Basic concepts in CFD

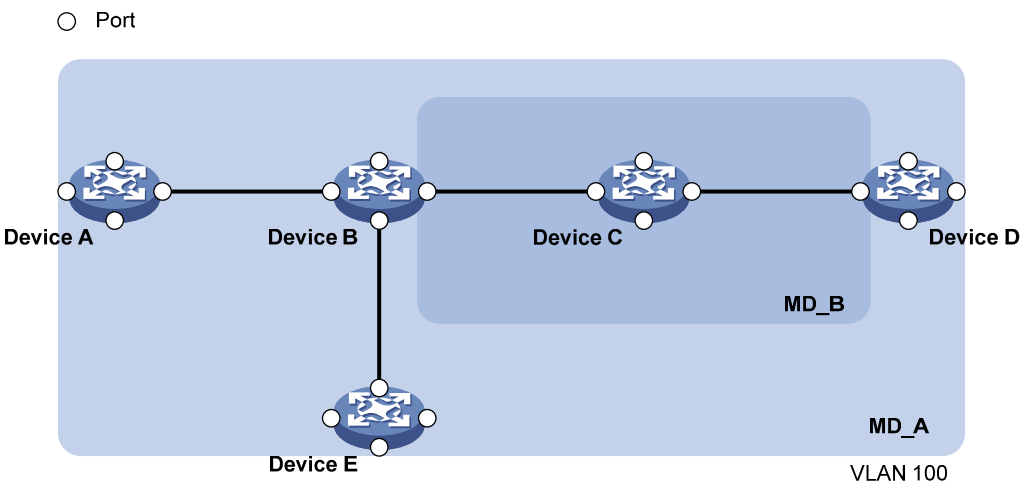
Maintenance domain

A maintenance domain (MD) defines the network where CFD plays its role. The MD boundary is defined by some maintenance association end points (MEPs) configured on the ports. An MD is identified by an MD name.

To accurately locate faults, CFD assigns 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 3, MD_A in light blue nests MD_B in dark blue. If a connectivity fault is detected at the boundary of MD_A, any of the devices in MD_A, including Device A through Device E, may fail. If a connectivity fault is also detected at the boundary of MD_B, the failure points may be any of Device B through Device D. If the devices in MD_B can operate properly, at least Device C is operational.

Figure 3 Two nested MDs



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

Maintenance association

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

An MA serves a VLAN. Packets sent by the MPs in an MA carry the relevant VLAN tag. An MP can receive packets sent by other MPs in the same MA.

Maintenance point

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

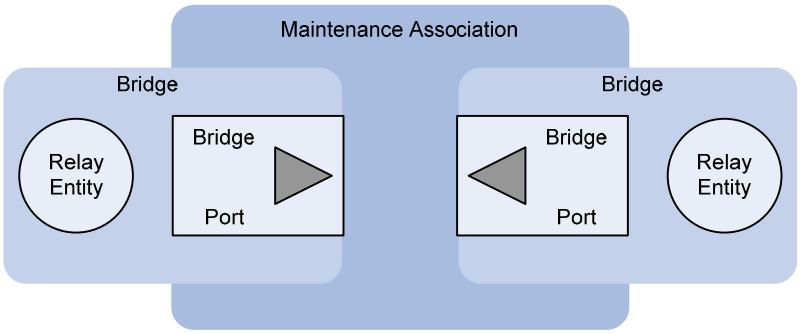
- MEP

Each MEP is identified by an integer called a "MEP ID". The MEPs of an MD define the range and boundary of the MD. The MA and MD that a MEP belongs to define the VLAN attribute and level of the packets sent by the MEP. MEPs are categorized as inward-facing MEPs and outward-facing MEPs.

The level of a MEP determines the levels of packets that the MEP can process. The packets transmitted from a MEP carry the level of the MEP. A MEP forwards packets at a higher level and processes packet of its own level or lower. The processing procedure is specific to packets in the same VLAN. Packets of different VLANs are independent.

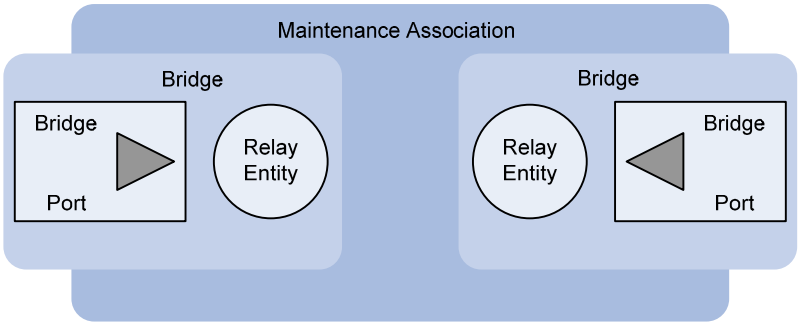
The direction of a MEP (outward-facing or inward-facing) determines the position of the MD relative to the port.

Figure 4 Outward-facing MEP



As shown in Figure 4, an outward-facing MEP sends packets to its host port.

Figure 5 Inward-facing MEP



As shown in Figure 5, an inward-facing MEP does not send packets to its host port. Rather, it sends packets to other ports on the device.

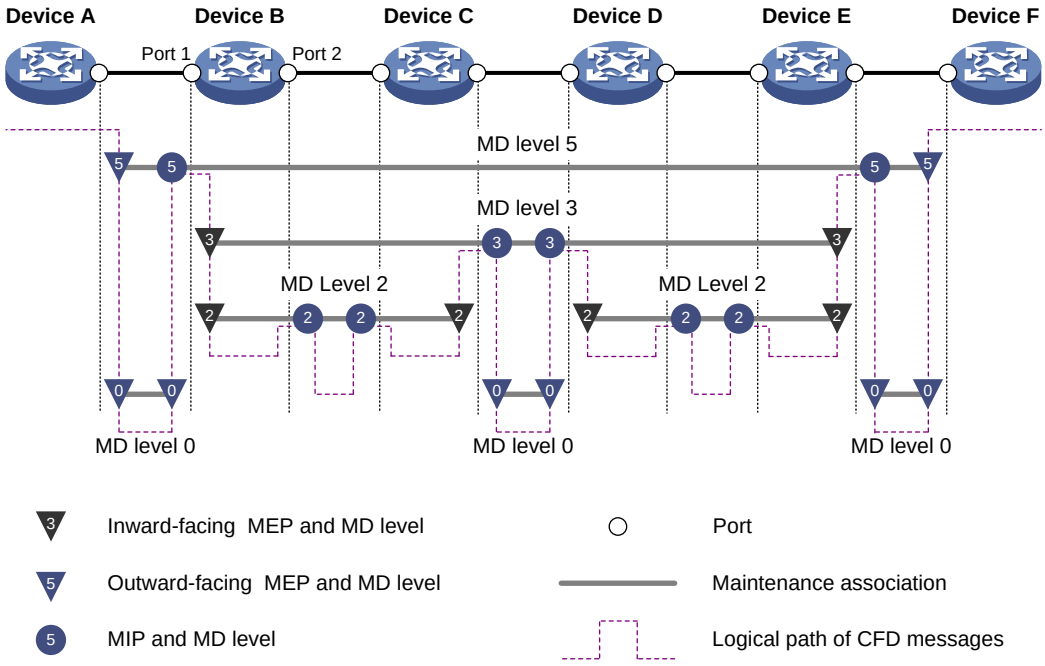
- MIP

A MIP is internal to an MD. It cannot send CFD packets actively; however, it can handle and respond to CFD packets. The MA and MD to which a MIP belongs define the VLAN attribute and level of the packets received.

By cooperating with MEPs, a MIP can perform a function similar to ping and traceroute. Like a MEP, a MIP forwards packets at a higher level without any processing and only processes packet of its own level or lower.

Figure 6 demonstrates a grading example of the CFD module. Six devices labeled A through F respectively exist. Suppose each device has two ports, and MEPs and MIPs are configured on some of these ports. Four levels of MDs are designed in this example; the bigger the number, the higher the level and the larger the area covered. In this example, Port 1 of device B is configured with the following MPs—a level 5 MIP, a level 3 inward-facing MEP, a level 2 inward-facing MEP, and a level 0 outward-facing MEP.

Figure 6 Levels of MPs



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) that carries a MEP ID not included in the MEP list of the MA, it drops the message.

CFD functions

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

- Continuity check (CC)

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

CC

Connectivity faults are usually caused by device faults or configuration errors. CC checks the connectivity between MEPs. This function is implemented through periodic sending of CCMs by the MEPs. As a multicast message, 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.

LB

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

LT

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

AIS

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

LM

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

DM

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

1. One-way frame delay measurement

The source MEP sends a one-way delay measurement (1DM) frame, which carries the transmission time, to the target MEP. Upon receiving the 1DM frame, the target MEP records the reception time, and

calculates and records the link transmission delay and jitter (delay variation) according to the transmission time and reception time. 1DM frames are multicast frames.

2. Two-way frame delay measurement

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

TST

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

Protocols and standards

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

CFD configuration task list

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

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

Complete the following tasks to configure CFD:

Tasks			Remarks
Configuring basic CFD settings	Enabling CFD		Required
	Configuring the CFD protocol version		Optional
	Configuring service instances	Creating a service instance with the MD name	Required Perform either task
		Creating a service instance without the MD name	
	Configuring MEPs		Required
	Configuring MIP generation rules		Required

Tasks		Remarks
Configuring CFD functions	Configuring CC on MEPs	Required
	Configuring LB on MEPs	Optional
	Configuring LT on MEPs	Optional
	Configuring AIS	Optional
	Configuring LM	Optional
	Configuring one-way DM	Optional
	Configuring two-way DM	Optional
	Configuring TST	Optional

NOTE:

A port blocked by STP 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.

Configuring basic CFD settings

Enabling CFD

Enable CFD on all concerned devices.

Follow these steps to enable CFD on a device:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable CFD	**cfd enable**	Required Disabled by default.

Configuring the CFD protocol version

Three CFD protocol versions are available: IEEE 802.1ag draft5.2 version, IEEE 802.1ag draft5.2 interim version, and IEEE 802.1ag standard version. Devices in a same MD must use the same CFD protocol version; otherwise, they cannot exchange CFD protocol packets.

Follow these steps to configure the CFD protocol version:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure the CFD protocol version	**cfd version** { **draft5** | **draft5-plus** | **standard** }	Optional By default, CFD uses the standard version of IEEE 802.1ag.

Configuring service instances

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

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

Service instances fall into two types:

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

You can create either type of service instance as needed.

Creating a service instance with the MD name

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

Follow these steps in strict order to configure a service instance with the MD name:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Create an MD	**cfd md** *md-name* **level** *level-value*	Required Not created by default.
Create an MA	**cfd ma** *ma-name* **md** *md-name* **vlan** vlan-id	Required Not created by default.
Create a service instance with the MD name	**cfd service-instance** *instance-id* **md** *md-name* **ma** *ma-name*	Required Not created by default.

CAUTION:

You must create the MD, MA, and service instance by strictly following the order stated in the table.

Creating a service instance without the MD name

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

Follow these steps to create a service instance without the MD name:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Create a service instance without the MD name	**cfd service-instance** *instance-id* **maid format** { **icc-based** *ma-name* | **string** *ma-name* } **level** *level-value* **vlan** *vlan-id*	Required Not created by default.

Configuring MEPs

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

Before creating MEPs, configure the MEP list first. An MEP list is a collection of local MEPs allowed to be configured in an MA and the remote MEPs to be monitored.

Follow these steps to configure a MEP:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure a MEP list	**cfd meplist** *mep-list* **service-instance** *instance-id*	Required By default, no MEP list is configured.
Enter Ethernet interface view	**interface** *interface-type interface-number*	—
Create a MEP	**cfd mep** *mep-id* **service-instance** *instance-id* { **inbound** | **outbound** }	Required Not configured by default.
Enable the MEP	**cfd mep service-instance** *instance-id* **mep** *mep-id* **enable**	Required Disabled by default.

NOTE:

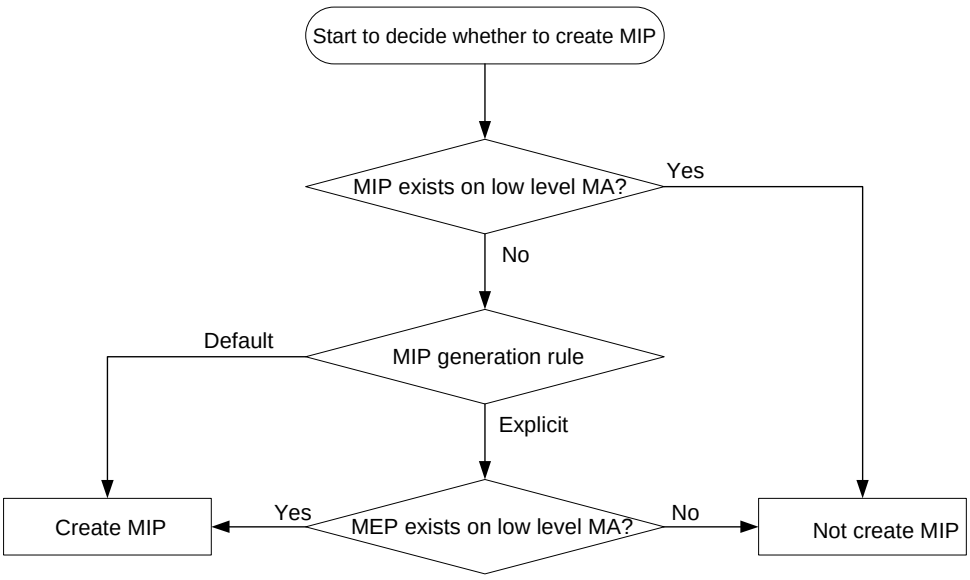
You cannot create a MEP if the MEP ID is not included in the MEP list of the service instance.

Configuring MIP generation rules

As functional entities in a service instance, MIPs respond to various CFD frames, such as LTM frames, LBM frames, 1DM frames, DMM frames, and TST frames.

MIPs are generated on each port automatically according to related MIP generation rules. If a port has no MIP, the system will check the MAs in each MD (from low to high levels), and follow the process shown in Figure 7 to create or not to create MIPs (within the same VLAN):

Figure 7 Process of creating MIPs



You can choose appropriate MIP generation rules based on your network design.

Follow these steps to configure the rules for generating MIPs:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure the rules for generating MIPs	**cfd mip-rule** { **explicit** | **default** } **service-instance** *instance-id*	Required By default, neither MIPs nor the rules for generating MIPs are configured.

CAUTION:

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

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

Configuring CFD functions

Configuration prerequisites

Before configuring CFD functions, you need to complete basic CFD configurations first.

Configuring CC on MEPs

After the CC function is configured, MEPs can send CCM frames to one another to check the connectivity between them.

You must configure CC before configuring other CFD functions.

Follow these steps to configure CC on a MEP:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure the interval field value in the CCM messages sent by MEPs	**cfd cc interval** *interval-value* **service-instance** *instance-id*	Optional By default, the interval field value is 4.
Enter Ethernet interface view	**interface** *interface-type interface-number*	—
Enable CCM sending on a MEP	**cfd cc service-instance** *instance-id* **mep** *mep-id* **enable**	Required Disabled by default.

CAUTION:

On different devices, the MEPs belonging to the same MD and MA should be configured with the same CCM transmission interval.

The relationship between the interval field value in the CCM messages, the interval between CCM messages and the timeout time of the remote MEP is illustrated in Table 9.

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

Interval field value	Interval between CCM messages	Timeout time of the remote MEP
4	1 second	3.5 seconds
5	10 second	35 seconds
6	60 seconds	210 seconds
7	600 seconds	2100 seconds

Configuring LB on MEPs

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

Follow these steps to configure LB on a MEP:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable LB	**cfd loopback service-instance** *instance-id* **mep** *mep-id* { **target-mep** *target-mep-id* | **target-mac** *mac-address* } [**number** *number*]	Required Disabled by default

Configuring LT on MEPs

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

- To trace the path between the source MEP and target MEPs
  - The source MEP first sends LTM messages to the target MEP.
  - Based on the LTR messages in response to the LTM messages, the path between the two MEPs can be identified.
- To locate link faults by sending LT messages automatically
  - After LT messages automatic sending is enabled, if the source MEP fails to receive the CCM frames from the target MEP within 3.5 times the transmission interval, the link between the two is considered faulty and LTM frames—with the target MEP as the destination and the TTL field in the LTM frames set to the maximum value 255—will be sent out.
  - Based on the LTRs that the MIPs return, the fault source can be located.

Follow these steps to configure LT on MEPs:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Find the path between a source MEP and a target MEP	**cfd linktrace service-instance** *instance-id* **mep** *mep-id* { **target-mep** *target-mep-id* | **target-mac** *mac-address* } [**ttl** *ttl-value*] [**hw-only**]	Required

To do...	Use the command...	Remarks
Enable LT messages automatic sending	**cfd linktrace auto-detection** [**size** *size-value*]	Required Disabled by default.

Configuring AIS

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

Follow these steps to configure AIS:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable AIS	**cfd ais enable**	Required Disabled by default.
Configure the AIS frame transmission level	**cfd ais level** *level-value* **service-instance** *instance-id*	Required Not configured by default.
Configure the AIS frame transmission interval	**cfd ais period** *period-value* **service-instance** *instance-id*	Optional 1 second by default.

NOTE:

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

Configuring LM

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

Follow these steps to configure LM:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure LM	**cfd slm service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]	Required Disabled by default.

CAUTION:

The LM function takes effect only in CFD IEEE 802.1ag.

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.

Follow these steps to configure one-way DM:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure one-way DM	**cfd dm one-way service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]	Required Disabled by default.

CAUTION:

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

Configuring two-way DM

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

Follow these steps to configure two-way DM:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure two-way DM	**cfd dm two-way service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]	Required Disabled by default.

CAUTION:

The two-way DM function is available only under the IEEE 802.1ag standard version of CFD.

Configuring TST

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

Follow these steps to configure TST:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure TST	**cfd tst service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*] [**length-of-test** *length*] [**pattern-of-test** { **all-zero** | **prbs** } [**with-crc**]]	Required Disabled by default.

CAUTION:

- The TST function takes effect only in CFD IEEE 802.1ag.
- To view the test result, use the **display cfd tst** command on the target MEP.

Displaying and maintaining CFD

To do...	Use the command...	Remarks
Display CFD and AIS status	**display cfd status** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the CFD protocol version	**display cfd version** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display MD configuration information	**display cfd md** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display MA configuration information	**display cfd ma** [[*ma-name*] **md** { *md-name* | **level** *level-value* }] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display service instance configuration information	**display cfd service-instance** [*instance-id*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display MEP list in a service instance	**display cfd meplist** [**service-instance** *instance-id*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display MP information	**display cfd mp** [**interface** *interface-type interface-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the attribute and running information of the MEPs	**display cfd mep** *mep-id* **service-instance** *instance-id* [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display LTR information received by a MEP	**display cfd linktrace-reply** [**service-instance** *instance-id* [**mep** *mep-id*]] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the information of a remote MEP	**display cfd remote-mep service-instance** *instance-id* **mep** *mep-id* [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the content of the LTR messages received as responses to the automatically sent LTMs	**display cfd linktrace-reply auto-detection** [**size** *size-value*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the AIS configuration and information on the specified MEP	**display cfd ais** [**service-instance** *instance-id* [**mep** *mep-id*]] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the one-way DM result on the specified MEP	**display cfd dm one-way history** [**service-instance** *instance-id* [**mep** *mep-id*]] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

To do...	Use the command...	Remarks
Display the TST result on the specified MEP	**display cfd tst** [**service-instance** *instance-id* [**mep** *mep-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear the one-way DM result on the specified MEP	**reset cfd dm one-way history** [**service-instance** *instance-id* [**mep** *mep-id*]]	Available in user view
Clear the TST result on the specified MEP	**reset cfd tst** [**service-instance** *instance-id* [**mep** *mep-id*]]	Available in user view

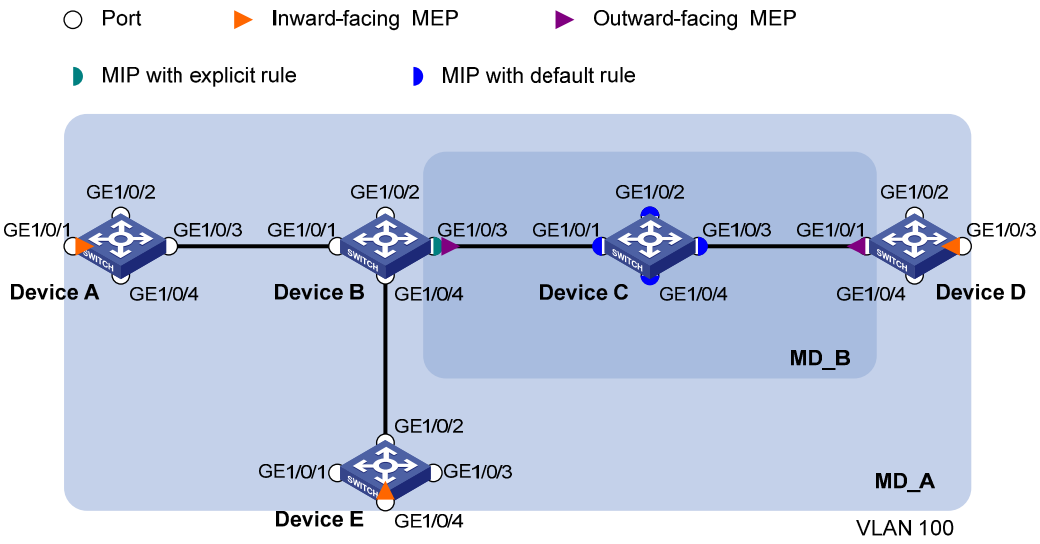
CFD configuration example

Network requirements

As shown in Figure 8:

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

Figure 8 Network diagram for CFD configuration



Configuration procedure

1. Configure a VLAN and assign ports to it

On each device shown in Figure 8, create VLAN 100 and assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to VLAN 100.

2. Enable CFD

Enable CFD on Device A.

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

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

3. Configure service instances

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

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

Configure Device E as you configure Device A.

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

```
[DeviceB] cfd md MD_A level 5
[DeviceB] cfd ma MA_A md MD_A vlan 100
[DeviceB] cfd service-instance 1 md MD_A ma MA_A
[DeviceB] cfd md MD_B level 3
[DeviceB] cfd ma MA_B md MD_B vlan 100
[DeviceB] cfd service-instance 2 md MD_B ma MA_B
```

Configure Device D as you configure Device B.

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

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

4. Configure MEPs

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

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

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

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

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

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

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

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

5. Configure MIPs

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

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

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

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

6. Configure CC

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

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

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

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

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

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

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

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

7. Configure AIS

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

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

Verify the configurations

1. Verify the LB function

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

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

```
[DeviceA] cfd loopback service-instance 1 mep 1001 target-mep 5001
Loopback to 0010-FC00-6515 with the sequence number start from 1001-43404:
Reply from 0010-FC00-6515: sequence number=1001-43404
Reply from 0010-FC00-6515: sequence number=1001-43405
Reply from 0010-FC00-6515: sequence number=1001-43406
Reply from 0010-FC00-6515: sequence number=1001-43407
Reply from 0010-FC00-6515: sequence number=1001-43408
Send:5        Received:5        Lost:0
```

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

2. Verify the LT function

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

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

3. Verify the LM function

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

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

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

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

4. Verify the one-way DM function

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

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

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

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

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

5. Verify the two-way DM function

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

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

```
[DeviceA] cfd dm two-way service-instance 1 mep 1001 target-mep 4002
```

```
Frame delay:
Reply from 0010-FC00-6514: 10ms
Reply from 0010-FC00-6514: 9ms
Reply from 0010-FC00-6514: 11ms
Reply from 0010-FC00-6514: 5ms
Reply from 0010-FC00-6514: 5ms
Average: 8ms
Send DMM frames: 5       Received: 5        Lost: 0

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

6. Verify the TST function

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

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

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

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

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

DLDP configuration

This chapter includes these topics:

- Overview
- DLDP configuration task list
- Displaying and maintaining DLDP
- DLDP configuration examples
- Troubleshooting DLDP

Overview

Background

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

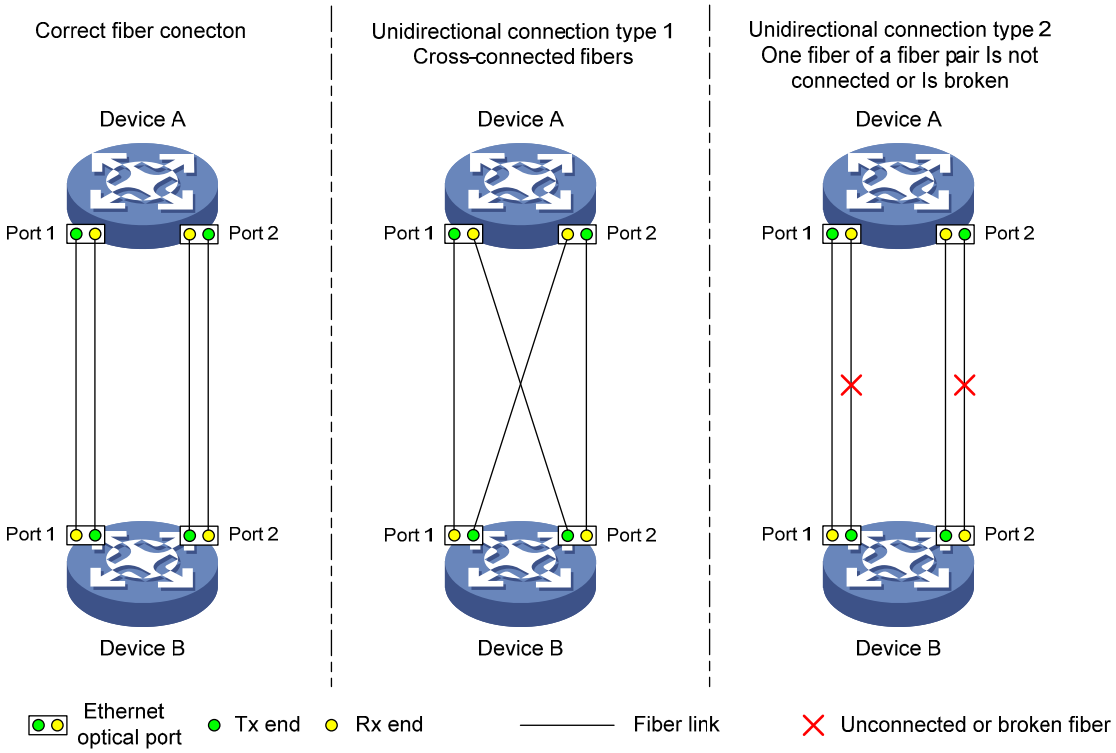
For example, the link between two switches, Switch A and Switch B, is a bidirectional link when they are connected via a fiber pair, with one fiber used for sending packets from A to B and the other for sending packets from B to A. This link is a two-way link. If one of the fibers gets broken, the link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

Unidirectional fiber links fall into the following types.

- One type occurs when fibers are cross-connected.
- The other type occurs when a fiber is not connected at one end, or when one fiber of a fiber pair gets broken.

Figure 9 shows a correct fiber connection and the two types of unidirectional fiber connection.

Figure 9 Correct and incorrect fiber connections



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

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

How DLDP works

DLDP link states

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

Table 10 DLDP link states

State	Indicates…
Initial	DLDP is disabled.
Inactive	DLDP is enabled, and the link is down.
Active	DLDP is enabled and the link is up, or the neighbor entries have been cleared.

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

DLDP timers

Table 11 DLDP timers

DLDP timer	Description
Active timer	Determines the interval for sending Advertisement packets with RSY tags, which defaults to 1 second. By default, a switch in the active DLDP link state sends one Advertisement packet with RSY tags every second. The maximum number of advertisement packets with RSY tags that can be sent successively is 5.
Advertisement timer	Determines the interval for sending common advertisement packets, which defaults to 5 seconds.
Probe timer	Determines the interval for sending Probe packets, which defaults to 1 second. By default, a switch in the probe state sends one Probe packet every second. The maximum number of Probe packets that can be sent successively is 10.
Echo timer	This timer is set to 10 seconds. It is triggered when a switch transits to the Probe state or when an enhanced detect is launched. When the Echo timer expires and no Echo packet has been received from a neighbor device, the state of the link is set to unidirectional and the switch transits to the Disable state. In this case, the switch does the following: • Sends Disable packets. • Either prompts the user to shut down the port or shuts down the port automatically (depending on the DLDP down mode configured). • Removes the corresponding neighbor entries.
Entry timer	When a new neighbor joins, a neighbor entry is created and the corresponding entry timer is triggered. When a DLDP packet is received, the switch updates the corresponding neighbor entry and the entry timer. In normal mode, if no packet is received from a neighbor when the corresponding entry timer expires, DLDP sends advertisement packets with RSY tags and removes the neighbor entry. In enhanced mode, if no packet is received from a neighbor when the Entry timer expires, DLDP triggers the enhanced timer. The setting of an Entry timer is three times that of the Advertisement timer.

DLDP timer	Description
Enhanced timer	In enhanced mode, this timer is triggered if no packet is received from a neighbor when the entry timer expires. Enhanced timer is set to 1 second. After the Enhanced timer is triggered, the switch sends up to eight probe packets to the neighbor at a frequency of one packet per second.
DelayDown timer	A switch in Active, Advertisement, or Probe DLDP link state transits to DelayDown state rather than removes the corresponding neighbor entry and transits to the Inactive state when it detects a port-down event. When a switch transits to this state, the DelayDown timer is triggered. A switch in DelayDown state only responds to port-up events. If the switch in the DelayDown state detects a port-up event before the DelayDown timer expires, it resumes its original DLDP state. If not, when the DelayDown timer expires, the switch removes the corresponding DLDP neighbor information and transits to the Inactive state.
RecoverProbe timer	This timer is set to 2 seconds. A port in the Disable state sends one RecoverProbe packet every two seconds to detect whether a unidirectional link has restored.

DLDP mode

DLDP can operate in normal or enhanced mode.

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

Table 12 DLDP mode and neighbor entry aging

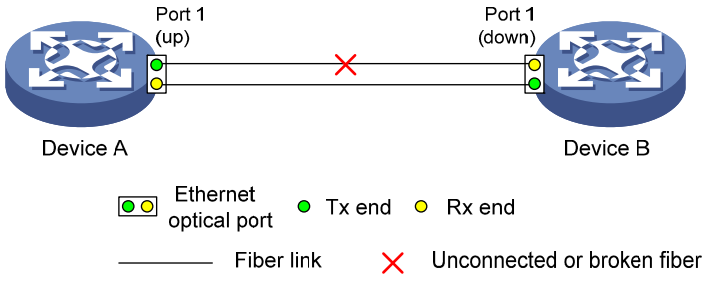
DLDP mode	Detecting a neighbor after the corresponding neighbor entry ages out	Removing the neighbor entry immediately after the Entry timer expires	Triggering the Enhanced timer after an Entry timer expires
Normal DLDP mode	No	Yes	No
Enhanced DLDP mode	Yes	No	Yes

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

If you configure forced speed and full duplex mode on a port, the situation shown in Figure 10 may occur, where the port on Device B is actually down but its state cannot be detected by common data link protocols, so the port on Device A is still up. However, in enhanced DLDP mode, the following occurs:

1. The port on Device B is in Inactive DLDP state because it is physically down.
2. The port on Device A tests the peer port on Device B after the Entry timer for the port on Device B expires.
3. The port on Device A transits to the Disable state if it does not receive an Echo packet from the port on Device B when the Echo timer expires.

Figure 10 A scenario for enhanced DLDP mode



NOTE:

- In normal DLDP mode, only fiber cross-connected unidirectional links can be detected.
- In enhanced DLDP mode, the following types of unidirectional links can be detected: fiber cross-connected links, and fiber pairs with one fiber or broken or not connected. When a fiber of a fiber pair is broken or not connected, the port that can receive optical signals is in Disable state, and the other port is in Inactive state.

DLDP authentication mode

You can use DLDP authentication to prevent network attacks and illegal detecting. The following DLDP authentication modes are available.

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

DLDP processes

1. On a DLDP-enabled link that is in up state, DLDP sends DLDP packets to the peer device and processes the DLDP packets received from the peer device. DLDP packets sent vary with DLDP states. Table 13 lists DLDP states and their packet types.

Table 13 DLDP packet types and DLDP states

DLDP state	Type of DLDP packets sent
Active	Advertisement packet with RSY tag

DLDP state	Type of DLDP packets sent
Advertisement	Normal Advertisement packet
Probe	Probe packet
Disable	Disable packet and then RecoverProbe packet

NOTE:

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

2. A received DLDP packet is processed with the following methods.

- In any of the three authentication modes, the packet is dropped if it fails to pass the authentication.
- The packet is dropped if the setting of the interval to send Advertisement packets it carries conflicts with the corresponding local setting.
- Other processes are as shown in Table 14.

Table 14 Procedures for processing different types of DLDP packets received

Packet type	Processing procedure		
Advertisement packet with RSY tag	Retrieves the neighbor information	If the corresponding neighbor entry does not exist, creates the neighbor entry, triggers the Entry timer, and transits to Probe state.	
		If the corresponding neighbor entry already exists, resets the Entry timer and transits to Probe state.	
Normal Advertisement packet	Retrieves the neighbor information	If the corresponding neighbor entry does not exist, creates the neighbor entry, triggers the Entry timer, and transits to Probe state.	
		If the corresponding neighbor entry already exists, resets the Entry timer.	
Flush packet	Determines whether or not the local port is in Disable state	If yes, no process is performed.	
		If not, removes the corresponding neighbor entry (if any).	
Probe packet	Retrieves the neighbor information	If the corresponding neighbor entry does not exist, creates the neighbor entry, transits to Probe state, and returns Echo packets.	
		If the corresponding neighbor entry already exists, resets the Entry timer and returns Echo packets.	
Echo packet	Retrieves the neighbor information	If the corresponding neighbor entry does not exist, creates the neighbor entry, triggers the Entry timer, and transits to Probe state.	
		The corresponding neighbor entry already exists	If the neighbor information it carries conflicts with the corresponding locally maintained neighbor entry, drops the packet.
			Otherwise, sets the flag of the neighbor as two-way connected. In addition, if the flags of all the neighbors are two-way connected, the switch transits from Probe state to Advertisement state and disables the Echo timer.

Packet type	Processing procedure	
Disable packet	Checks whether the local port is in Disable state	If yes, no process is performed.
		If not, the local port transits to Disable state.
RecoverProbe packet	Checks whether the local port is in Disable or Advertisement state	If not, no process is performed.
		If yes, returns RecoverEcho packets.
RecoverEcho packet	Checks whether the local port is in Disable state	If not, no process is performed.
		If yes, the local port transits to Active state if the neighbor information the packet carries is consistent with the local port information.
LinkDown packet	Checks whether the local port operates in Enhanced mode	If not, no process is performed.
		If yes and the local port is not in Disable state, the local port transits to Disable state.

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

Table 15 DLDP process when no echo packet is received from the neighbor

No echo packet received from the neighbor	Processing procedure
In normal mode, no echo packet is received when the Echo timer expires.	DLDP transits to the Disable state, outputs log and tracking information, and sends Disable packets. In addition, depending on the user-defined DLDP down mode, DLDP shuts down the local port or prompts users to shut down the port, and removes the corresponding neighbor entry.
In enhanced mode, no echo packet is received when the Echo timer expires.	

Link auto-recovery mechanism

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

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

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

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

DLDP neighbor state

A DLDP neighbor can be in one of the three states described in Table 16.

Table 16 Description on DLDP neighbor states

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

DLDP configuration task list

Complete the following tasks to configure DLDP:

Task	Remarks
Enabling DLDP	Required
Setting DLDP mode	Optional
Setting the interval for sending advertisement packets	Optional
Setting the DelayDown timer	Optional
Setting the port shutdown mode	Optional
Configuring DLDP authentication	Optional
Resetting DLDP state	Optional

CAUTION:

- To ensure that DLDP works properly on a link, you must configure the full duplex mode for the ports at two ends of the link, and configure a speed for the two ports, rather than letting them negotiate a speed. For more information about the **duplex** and **speed** commands, see the *Layer 2—LAN Switching Command Reference*.
- For DLDP to work properly, enable DLDP on both sides and make sure these settings are consistent: the interval to send Advertisement packets, DLDP authentication mode, and password.
- DLDP does not process any link aggregation control protocol (LACP) events. The links in an aggregation are treated as individual links in DLDP.
- For DLDP to operate properly, make sure the DLDP version running on devices on the two sides are the same.

Enabling DLDP

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

Follow these steps to enable DLDP:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

To do…		Use the command…	Remarks
Enable DLDP globally		**dldp enable**	Required Globally disabled by default
Enter Ethernet port view or port group view	Enter Ethernet port view	**interface** *interface-type interface-number*	Either of the two is required. Configurations made in Ethernet port view apply to the current port only; configurations made in port group view apply to all ports in the port group.
	Enter port group view	**port-group manual** *port-group-name*	
Enable DLDP		**dldp enable**	Required Disabled on a port by default

NOTE:

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

Setting DLDP mode

DLDP works in normal or enhanced mode:

- In normal mode, DLDP does not actively detect neighbors when the corresponding neighbor entries age out. The system can identify only one type of unidirectional links: cross-connected fibers.
- In enhanced mode, DLDP actively detects neighbors when the corresponding neighbor entries age out, so the system can identify two types of unidirectional links: cross-connected fibers and disconnected fibers.

Follow these steps to set DLDP mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set DLDP mode	**dldp work-mode** { **enhance** | **normal** }	Optional Normal by default

Setting the interval for sending advertisement packets

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

Follow these steps to set the interval to send Advertisement packets:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the interval to send Advertisement packets	**dldp interval** *time*	Optional 5 seconds by default

NOTE:

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

Setting the DelayDown timer

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

Follow these steps to set the DelayDown timer

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the DelayDown timer	**dldp delaydown-timer** *time*	Optional 1 second by default

NOTE:

DelayDown timer setting applies to all DLDP-enabled ports.

Setting the port shutdown mode

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

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

Follow these steps to set port shutdown mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

To do…	Use the command…	Remarks
Set port shutdown mode	**dldp unidirectional-shutdown** { **auto** | **manual** }	Optional **auto** by default

NOTE:

- On a port with both remote OAM loopback and DLDP enabled, if the port shutdown mode is auto mode, the port will be shut down by DLDP when it receives a packet sent by itself, causing remote OAM loopback to operate improperly. To prevent this, set the port shutdown mode to manual mode.
- If the switch is busy, or the CPU usage is high, normal links may be treated as unidirectional links. In this case, you can set the port shutdown mode to manual mode to alleviate the impact caused by false unidirectional link report.

Configuring DLDP authentication

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

Follow these steps to configure DLDP authentication:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure DLDP authentication	**dldp authentication-mode** { **md5** *md5-password* | **none** | **simple** *simple-password* }	Required **none** by default

NOTE:

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

Resetting DLDP state

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

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

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

Resetting DLDP state in system view

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

Follow these steps to reset DLDP in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Reset DLDP state	**dldp reset**	Required

Resetting DLDP state in port view or port group view

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

Follow these steps to reset DLDP state in port view or port group view:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Enter Ethernet port view or port group view	Enter Ethernet port view	**interface** *interface-type interface-number*	Either is required. Configurations made in Ethernet port view apply to the current port only; configurations performed in port group view apply to all the ports in the port group.
	Enter port group view	**port-group manual** *port-group-name*	
Reset DLDP state		**dldp reset**	Required

Displaying and maintaining DLDP

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

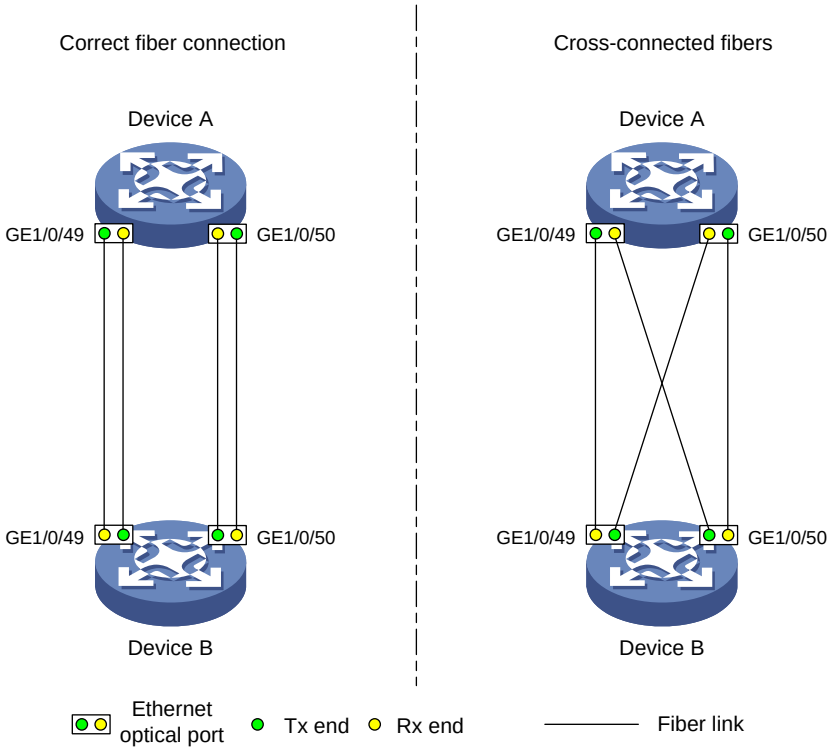
DLDP configuration examples

Automatically shutting down unidirectional links

Network requirements

- As shown in Figure 11, Device A and Device B are connected with two fiber pairs.
- Configure DLDP to automatically shut down the faulty port upon detecting a unidirectional link, and automatically bring up the port after you clear the fault.

Figure 11 Network diagram for configuring automatic shutdown of unidirectional links



Configuration procedure

1. Configuration on Device A

Enable DLDP globally.

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

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

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

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

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

Set the DLDP mode to enhanced.

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

Set the port shutdown mode to auto.

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

2. Configuration on Device B

Enable DLDP globally, configure GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 to operate in full duplex mode and at 1000 Mbps, and then enable DLDP on the two ports.

```
<DeviceB> system-view
[DeviceB] dldp enable
[DeviceB] interface gigabitethernet 1/0/49
[DeviceB-GigabitEthernet1/0/49] duplex full
[DeviceB-GigabitEthernet1/0/49] speed 1000
[DeviceB-GigabitEthernet1/0/49] dldp enable
[DeviceB-GigabitEthernet1/0/49] quit
[DeviceB] interface gigabitethernet 1/0/50
[DeviceB-GigabitEthernet1/0/50] duplex full
[DeviceB-GigabitEthernet1/0/50] speed 1000
[DeviceB-GigabitEthernet1/0/50] dldp enable
[DeviceB-GigabitEthernet1/0/50] quit
```

Set the DLDP mode to enhanced.

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

Set the port shutdown mode to auto.

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

3. Verifying the configurations

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

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

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

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

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

```
        Neighbor port index : 60
        Neighbor state : two way
        Neighbor aged time : 12
```

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

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

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

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

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

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

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

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

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

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

```
<DeviceA>
%Jan 18 17:47:33:869 2010 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/49 link status is UP.
%Jan 18 17:47:35:894 2010 DeviceA IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/50 link status is UP.
```

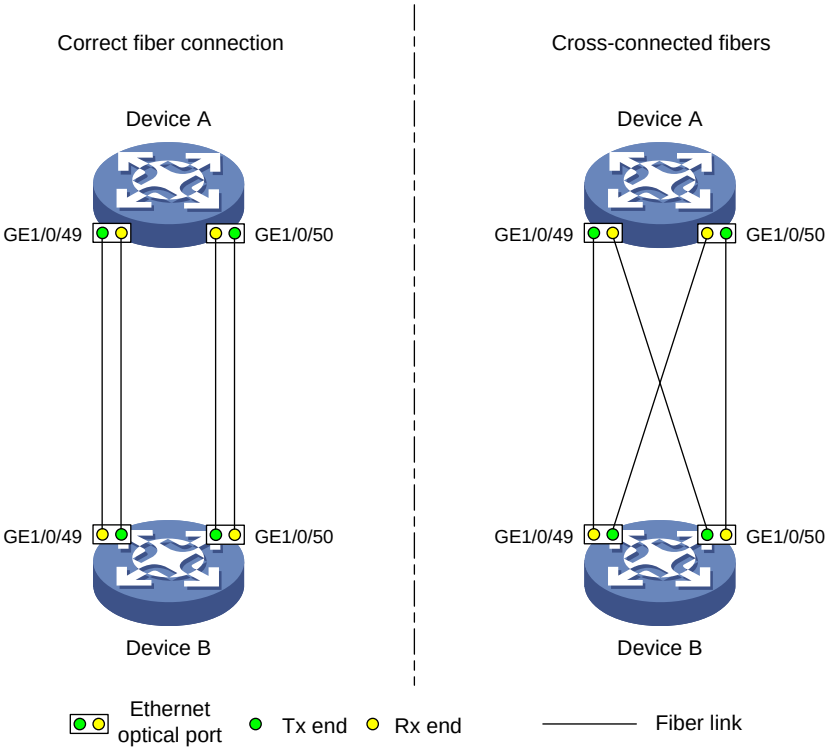
The output shows that the link status of both GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 is now up.

Manually shutting down unidirectional links

Network requirements

- As shown in Figure 12, Device A and Device B are connected with two fiber pairs.
- Configure DLDP to send information when a unidirectional link is detected, to remind the network administrator to manually shut down the faulty port.

Figure 12 Network diagram for configuring manual shutdown of unidirectional links



Configuration procedure

1. Configuration on Device A

Enable DLDP globally.

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

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

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

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

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

```
[DeviceA-GigabitEthernet1/0/50] dldp enable
[DeviceA-GigabitEthernet1/0/50] quit
```

Set the DLDP mode to enhanced.

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

Set the port shutdown mode to manual.

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

2. Configuration on Device B

Enable DLDP globally, configure GigabitEthernet 1/0/49 and GigabitEthernet 1/0/50 to operate in full duplex mode and at 1000 Mbps, and then enable DLDP on the two ports.

```
<DeviceB> system-view
[DeviceB] dldp enable
[DeviceB] interface gigabitethernet 1/0/49
[DeviceB-GigabitEthernet1/0/49] duplex full
[DeviceB-GigabitEthernet1/0/49] speed 1000
[DeviceB-GigabitEthernet1/0/49] dldp enable
[DeviceB-GigabitEthernet1/0/49] quit
[DeviceB] interface gigabitethernet 1/0/50
[DeviceB-GigabitEthernet1/0/50] duplex full
[DeviceB-GigabitEthernet1/0/50] speed 1000
[DeviceB-GigabitEthernet1/0/50] dldp enable
[DeviceB-GigabitEthernet1/0/50] quit
```

Set the DLDP mode to enhanced.

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

Set the port shutdown mode to manual.

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

3. Verifying the configurations

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Troubleshooting DLDP

Symptom

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

Analysis

The problem can be caused by the following.

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

Solution

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

Smart Link configuration

This chapter includes these sections:

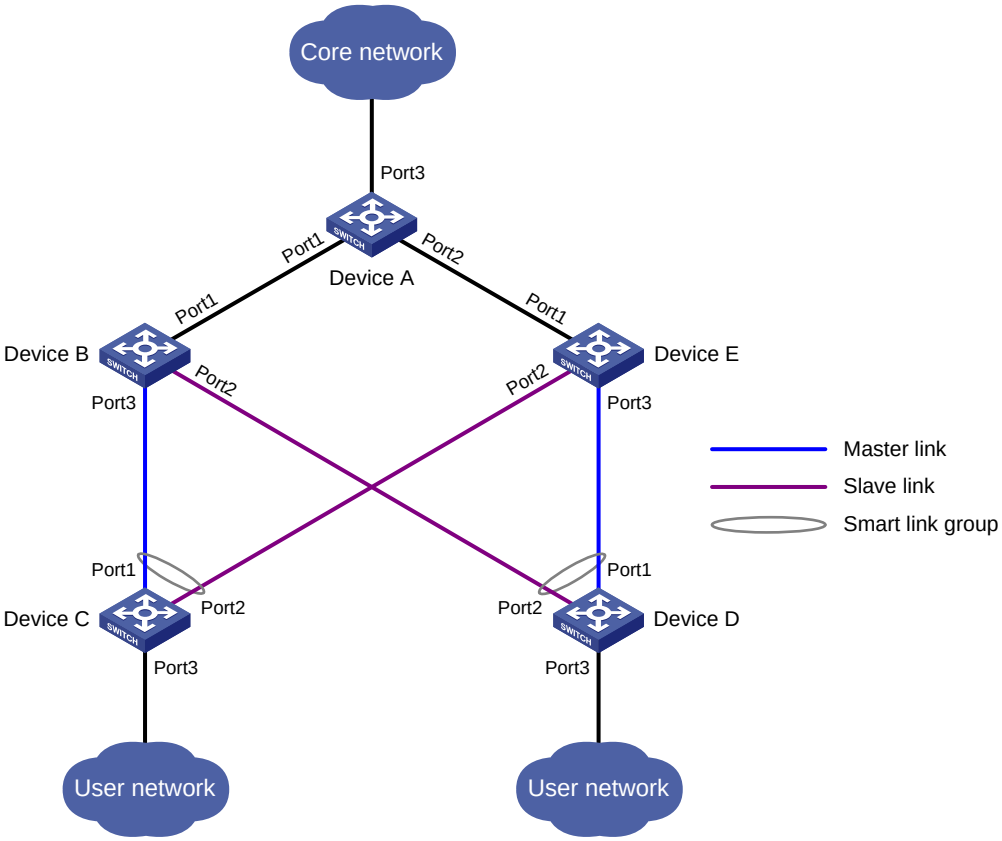
- Smart Link overview
- Configuring a smart link device
- Configuring an associated device
- Displaying and maintaining Smart Link
- Smart Link configuration examples

Smart Link overview

Background

To avoid single-point failures and guarantee network reliability, downstream devices are usually dual uplinked to upstream devices. As shown in Figure 13, a downstream device connects to two different upstream devices.

Figure 13 Diagram for a dual uplink network



A dual uplink network demonstrates high reliability, but it may contain network loops. In most cases, Spanning Tree Protocol (STP) is used to remove network loops. The problem with STP, however, is that STP

convergence time is long, which makes it not suitable for users who have high demand on convergence speed.

NOTE:

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

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

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

Terminology

Smart link group

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

As shown in Figure 13, Port1 and Port2 of Device C and Port1 and Port2 of Device D each form a smart link group, with Port1 being active and Port2 being standby.

Master port/slave port

Master port and slave port are two port roles in a smart link group. When both ports in a smart link group are up, the master port preferentially transitions to the forwarding state, and the slave port stays in the standby state. Once the master port fails, the slave port takes over to forward traffic. As shown in Figure 13, you can configure Port1 of Device C and that of Device D as master ports, and Port2 of Device C and that of Device D as slave ports.

Master link/slave link

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

Protected VLAN

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

Transmit control VLAN

The transmit control VLAN is used for transmitting flush messages. When link switchover occurs, the devices (such as Device C and Device D in Figure 13) broadcast flush messages within the transmit control VLAN.

Receive control VLAN

The receive control VLAN is used for receiving and processing flush messages. When link switchover occurs, the devices (such as Device A, Device B, and Device E in Figure 13) receive and process flush messages in the receive control VLAN and refresh their MAC address forwarding entries and ARP/ND entries.

Flush message

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

How Smart Link works

Link backup mechanism

As shown in Figure 13, the link on Port1 of Device C is the master link, and the link on Port2 of Device C is the slave link. Typically, Port1 is in the forwarding state, and Port2 is in the standby state. When the master link fails, Port2 takes over to forward traffic and Port1 is blocked and placed in the standby state.

NOTE:

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

Topology change mechanism

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

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

Role preemption mechanism

As shown in Figure 13, the link on Port1 of Device C is the master link, and the link on Port2 of Device C is the slave link. Once the master link fails, Port1 is automatically blocked and placed in the standby state, and Port2 takes over to forward traffic.

When the master link recovers:

- If the smart link group is not configured with role preemption, Port1 stays blocked, and no link switchover occurs, ensuring traffic stability. Port1 does not transition to the forwarding state until the next link switchover occurs.
- If the smart link group is configured with role preemption, Port1 takes over to forward traffic as soon as its link recovers, and Port2 is automatically blocked and placed in the standby state.

Load sharing mechanism

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

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

You can configure protected VLANs for a smart link group by referencing MSTIs.

Smart Link collaboration mechanisms

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

NOTE:

For more information about Monitor Link, see the chapter "Monitor link configuration."

Smart Link configuration task list

Complete the following tasks to configure Smart Link:

Task		Remarks
Configuring a smart link device	Configuring protected VLANs for a smart link group	Required
	Configuring member ports for a smart link group	Required
	Configuring role preemption for a smart link group	Optional
	Enabling the sending of flush messages	Optional
Configuring an associated device	Enabling the receiving of flush messages	Required

NOTE:

- A smart link device is a network device that supports Smart Link and is configured with a smart link group and a transmit control VLAN for flush message transmission. Device C and Device D in Figure 13 are two examples of smart link devices.
- An associated device is a network device that supports Smart Link, and receives flush messages sent from the specified control VLAN. Device A, Device B, and Device E in Figure 13 are examples of associated devices.

Configuring a smart link device

Configuration prerequisites

- Before configuring a port as a smart link group member, shut down the port to prevent loops. You can bring up the port only after completing the smart link group configuration.
- Disable STP on the ports you want to add to the smart link group, and make sure that the ports are not member ports of any aggregation group.

CAUTION:

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

Configuring protected VLANs for a smart link group

Follow these steps to configure the protected VLANs for a smart link group:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a smart link group and enter smart link group view	**smart-link group** *group-id*	—
Configure protected VLANs for the smart link group	**protected-vlan reference-instance** *instance-id-list*	Required By default, no protected VLAN is configured for a smart link group.

NOTE:

The **protected-vlan** command configures protected VLANs for a smart link group by referencing MSTIs. To view VLAN-to-MSTI mappings, use the **display stp region-configuration** command. For VLAN-to-MSTI mapping configuration, see the *Layer 2—LAN Switching Configuration Guide*.

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 port view. The configurations made in these two views have the same effect.

In smart link group view

Follow these steps to configure member ports for a smart link group in smart link group view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a smart link group and enter smart link group view	**smart-link group** *group-id*	—
Configure member ports for a smart link group	**port** *interface-type interface-number* { **master** | **slave** }	Required

In port view

Follow these steps to configure member ports for a smart link group in port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view or layer 2 aggregate port view	**interface** *interface-type interface-number*	—
Configure member ports for a smart link group	**port smart-link group** *group-id* { **master** | **slave** }	Required

Configuring role preemption for a smart link group

Follow these steps to configure role preemption for a smart link group:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a smart link group and enter smart link group view	**smart-link group** *group-id*	—
Enable role preemption	**preemption mode role**	Required Disabled by default
Configure the preemption delay	**preemption delay** *delay-time*	Optional 1 second by default

NOTE:

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

Enabling the sending of flush messages

Follow these steps to enable the sending of flush messages:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a smart link group and enter smart link group view	**smart-link group** *group-id*	Required
Enable flush update in the specified control VLAN	**flush enable** [**control-vlan** *vlan-id*]	Optional By default, flush update is enabled, and VLAN 1 is the control VLAN.

CAUTION:

- The control VLAN configured for a smart link group must be different from that configured for any other smart link group.
- Make sure that the configured control VLAN already exists, and assign the smart link group member ports to the control VLAN.
- The control VLAN of a smart link group should also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent properly.

Configuring an associated device

Configuration prerequisites

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

Enabling the receiving of flush messages

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

Follow these steps to enable the receiving of flush messages:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view or Layer 2 aggregate port view	**interface** *interface-type interface-number*	—
Configure the control VLANs for receiving flush messages	**smart-link flush enable** [**control-vlan** *vlan-id-list*]	Required By default, no control VLAN exists for receiving flush messages.

CAUTION:

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

Displaying and maintaining Smart Link

To do…	Use the command…	Remarks
Display smart link group information	**display smart-link group** { *group-id* | **all** } [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display information about the received flush messages	**display smart-link flush** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear the statistics about flush messages	**reset smart-link statistics**	Available in user view

Smart Link configuration examples

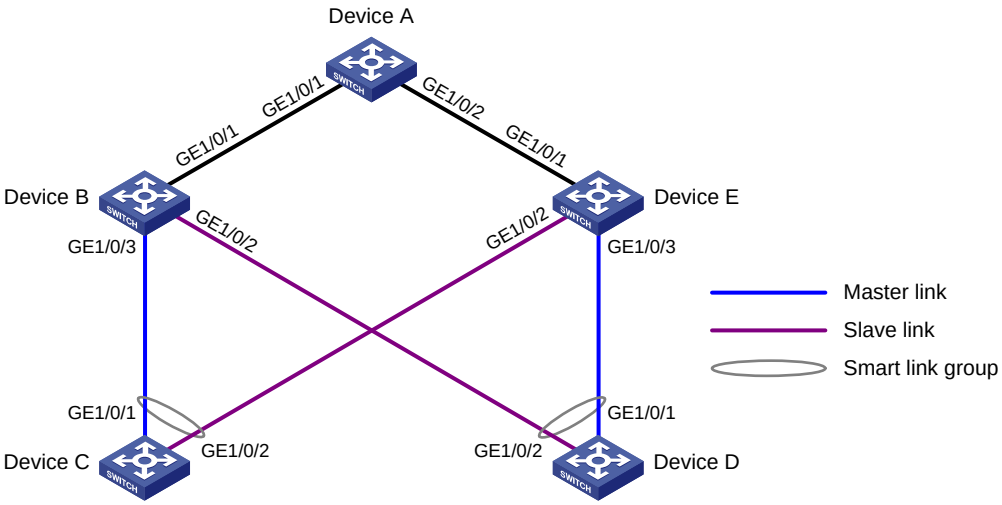
Single smart link group configuration example

Network requirements

As shown in Figure 14:

- Device C and Device D are smart link devices, and Device A, Device B, and Device E are associated devices. Traffic of VLANs 1 through 30 on Device C and Device D are dually uplinked to Device A.
- Configure Smart Link on Device C and Device D for dual uplink backup.

Figure 14 Network diagram for single smart link group configuration



Configuration procedure

1. Configuration on Device C

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

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

Shut down ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable STP on them, and configure them as trunk ports that permit VLANs 1 through 30.

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

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

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

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

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

In smart link group 1, enable flush message sending, and specify VLAN 10 as the control VLAN.

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

Bring up ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceC] interface gigabitethernet1/0/1
[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. Configuration on Device D

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

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

Shut down ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable STP on them, and configure them as trunk ports that permit VLANs 1 through 30.

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

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

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

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

```
[DeviceD-smlk-group1] port gigabitethernet 1/0/1 master
[DeviceD-smlk-group1] port gigabitethernet 1/0/2 slave
```

In smart link group 1, enable flush message sending, and specify VLAN 20 as the control VLAN.

```
[DeviceD-smlk-group1] flush enable control-vlan 20
[DeviceD-smlk-group1] quit
```

Bring up ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceD] interface gigabitethernet1/0/1
[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. Configuration on Device B

Create VLANs 1 through 30.

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

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 1 through 30. Enable flush message receiving on it, and configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 1 through 30. Disable the spanning tree feature and enable flush message receiving on it, and configure VLAN 20 as the receive control VLAN.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 20
[DeviceB-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLANs 1 through 30. Disable the spanning tree feature and enable flush message receiving on it, and configure VLAN 10 as the receive control VLAN.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] smart-link flush enable control-vlan 10
[DeviceB-GigabitEthernet1/0/3] quit
```

4. Configuration on Device E

Create VLANs 1 through 30.

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

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLANs 1 through 30. Enable flush message receiving on it, and configure VLAN 10 and VLAN 20 as the receive control VLANs.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
```

```
[DeviceE-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLANs 1 through 30. Disable the spanning tree feature and enable flush message receiving on it, and configure VLAN 10 as the receive control VLAN.

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10
[DeviceE-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLANs 1 through 30. Disable the spanning tree feature and enable flush message receiving on it, and configure VLAN 20 as the receive control VLAN.

```
[DeviceE] interface gigabitethernet 1/0/3
[DeviceE-GigabitEthernet1/0/3] port link-type trunk
[DeviceE-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/3] undo stp enable
[DeviceE-GigabitEthernet1/0/3] smart-link flush enable control-vlan 20
[DeviceE-GigabitEthernet1/0/3] quit
```

5. Configuration on Device A

Create VLANs 1 through 30.

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

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports that permit VLANs 1 through 30, enable flush message receiving on them, and specify VLAN 10 and VLAN 20 as the control VLANs for receiving flush messages.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/2] quit
```

6. Verifying the configurations

Use the **display smart-link group** command to display the smart link group configuration on each device. For example:

Display the smart link group configuration on Device C.

```
[DeviceC] display smart-link group 1
 Smart link group 1 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: NONE
 Preemption delay: 1(s)
 Control VLAN: 10
```

```
Protected VLAN: Reference Instance 1
Member                    Role    State    Flush-count Last-flush-time
--------------------------------------------------------------------------
GigabitEthernet1/0/1      MASTER  ACTVIE   5           16:37:20 2010/02/21
GigabitEthernet1/0/2      SLAVE   STANDBY  1           17:45:20 2010/02/21
```

You can use the **display smart-link flush** command to display the flush messages received on each device. For example:

Display the flush messages received on Device B.

```
[DeviceB] display smart-link flush
 Received flush packets                          : 5
 Receiving interface of the last flush packet    : GigabitEthernet1/0/3
 Receiving time of the last flush packet         : 16:25:21 2009/02/21
 Device ID of the last flush packet              : 000f-e23d-5af0
 Control VLAN of the last flush packet           : 10
```

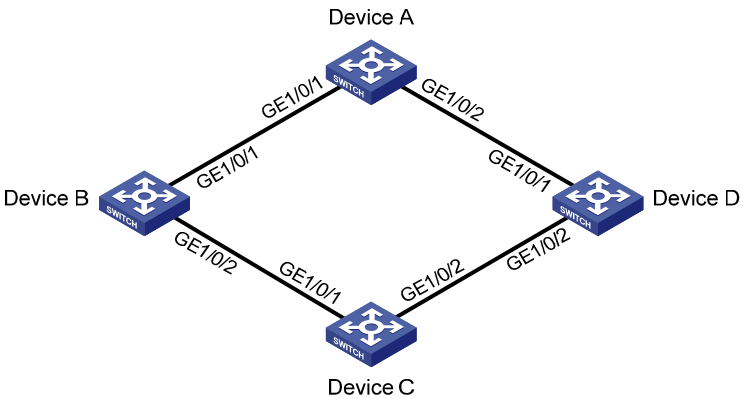
Multiple smart link groups load sharing configuration example

Network requirements

As shown in Figure 15:

- Device C is a smart link device, and Device A, Device B, and Device D are associated devices. Traffic of VLANs 1 through 200 on Device C are dually uplinked to Device A by Device B and Device D.
- Implement dual uplink backup and load sharing on Device C:
  - Traffic of VLANs 1 through 100 is uplinked to Device A by Device B.
  - Traffic of VLANs 101 through 200 is uplinked to Device A by Device D.

Figure 15 Network diagram for multiple smart link groups load sharing configuration



Configuration procedure

1. Configuration on Device C

Create VLAN 1 through VLAN 200, map VLANs 1 through 100 to MSTI 1, and VLANs 101 through 200 to MSTI 2, and activate MST region configuration.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 200
[DeviceC] stp region-configuration
```

```
[DeviceC-mst-region] instance 1 vlan 1 to 100
[DeviceC-mst-region] instance 2 vlan 101 to 200
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

Shut down ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, disable STP on them, and configure them as trunk ports that permit VLANs 1 through 200.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/2] quit
```

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

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

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

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

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

```
[DeviceC-smlk-group1] preemption mode role
[DeviceC-smlk-group-1] flush enable control-vlan 10
[DeviceC-smlk-group-1] quit
```

Create smart link group 2, and configure all VLANs mapped to MSTI 2 as the protected VLANs for smart link group 2.

```
[DeviceC] smart-link group 2
[DeviceC-smlk-group2] protected-vlan reference-instance 2
```

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

```
[DeviceC-smlk-group2] port gigabitethernet 1/0/2 master
[DeviceC-smlk-group2] port gigabitethernet 1/0/1 slave
```

Enable role preemption in smart link group 2, enable flush message sending, and configure VLAN 101 as the transmit control VLAN.

```
[DeviceC-smlk-group2] preemption mode role
[DeviceC-smlk-group2] flush enable control-vlan 101
[DeviceC-smlk-group2] quit
```

Bring up ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceC] interface gigabitethernet1/0/1
```

```
[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. Configuration on Device B

Create VLAN 1 through VLAN 200.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 200
```

Configure GigabitEthernet 1/0/1 as a trunk port and assign it to VLANs 1 through 200. Enable flush message receiving and configure VLAN 10 and VLAN 101 as the receive control VLANs on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 101
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port and assign it to VLANs 1 through 200. Disable the spanning tree feature and enable flush message receiving on it, and configure VLAN 10 and VLAN 101 as the receive control VLANs.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 101
[DeviceB-GigabitEthernet1/0/2] quit
```

3. Configuration on Device D

Create VLAN 1 through VLAN 200.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 200
```

Configure GigabitEthernet 1/0/1 as a trunk port and assign it to VLANs 1 through 200. Enable flush message receiving and configure VLAN 10 and VLAN 101 as the receive control VLANs on GigabitEthernet 1/0/1.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 101
[DeviceD-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port and assign it to VLANs 1 through 200. Disable the spanning tree feature and enable flush message receiving on it, and configure VLAN 10 and VLAN 101 as the receive control VLANs.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 101
```

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

4. Configuration on Device A

Create VLAN 1 through VLAN 200.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 200
```

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports and assign them to VLANs 1 through 200; enable flush message receiving on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 and configure VLAN 10 and VLAN 101 as the receive control VLANs.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 101
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 101
[DeviceA-GigabitEthernet1/0/2] quit
```

5. Verifying the configurations

Use the **display smart-link group** command to display the smart link group configuration on each device. For example:

Display the smart link group configuration on Device C.

```
[DeviceC] display smart-link group all
 Smart link group 1 information:
 Device ID: 000f-e23d-5af0
 Preemption delay: 1(s)
 Preemption mode: ROLE
 Control VLAN: 10
 Protected VLAN: Reference Instance 1
 Member                    Role    State    Flush-count Last-flush-time
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/1      MASTER  ACTVIE   5           16:37:20 2010/02/21
 GigabitEthernet1/0/2      SLAVE   STANDBY  1           17:45:20 2010/02/21

 Smart link group 2 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 101
 Protected VLAN: Reference Instance 2
 Member                    Role    State    Flush-count Last-flush-time
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/2      MASTER  ACTVIE   5           16:37:20 2010/02/21
 GigabitEthernet1/0/1      SLAVE   STANDBY  1           17:45:20 2010/02/21
```

Use the **display smart-link flush** command to display the flush messages received on each device. For example:

Display the flush messages received on Device B.

```
[DeviceB] display smart-link flush
 Received flush packets                              : 5
 Receiving interface of the last flush packet        : GigabitEthernet1/0/2
 Receiving time of the last flush packet             : 16:25:21 2010/02/21
 Device ID of the last flush packet                  : 000f-e23d-5af0
 Control VLAN of the last flush packet               : 10
```

Monitor Link configuration

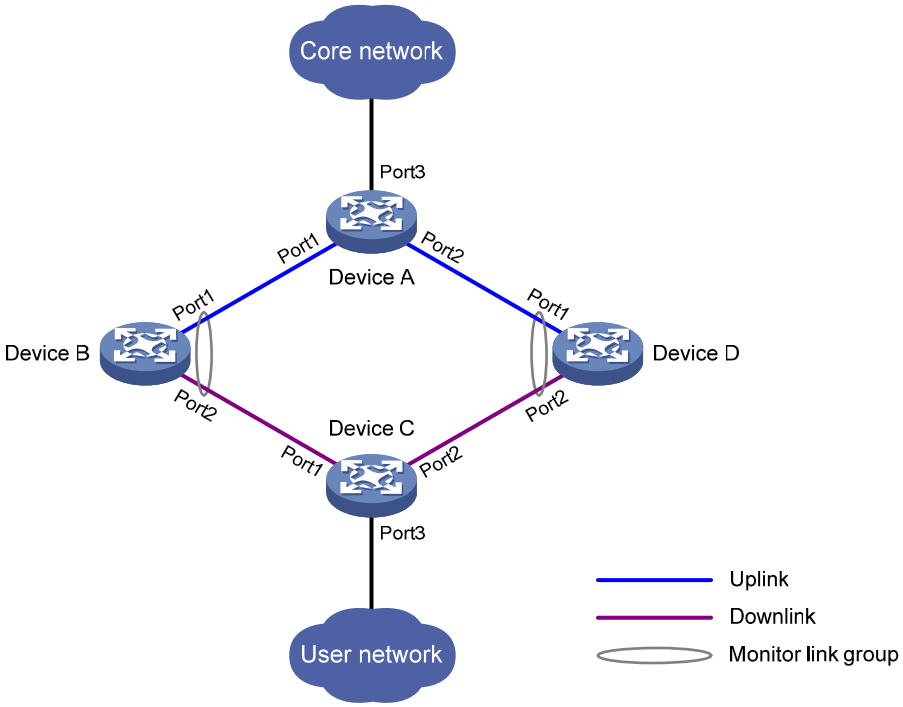
This chapter includes these sections:

- Overview
- Configuring Monitor Link
- Displaying and maintaining Monitor Link
- Monitor Link configuration example

Overview

Monitor Link is a port collaboration function. Monitor Link usually works together with Layer 2 topology protocols. The idea is to monitor the states of uplink ports and adapt the up/down state of downlink ports to the up/down state of uplink ports, triggering link switchover on the downstream device in time, as shown in Figure 16.

Figure 16 Monitor Link application scenario



Terminology

Monitor link group

A monitor link group is a set of uplink and downlink ports. A port can belong to only one monitor link group. As shown in Figure 16, ports Port1 and Port2 of Device B and those of Device D each form a monitor link group. Port1 on both devices are uplink ports, and Port2 on both devices are downlink ports.

Uplink/Downlink ports

Uplink port and downlink port are two port roles in monitor link groups:

- Uplink ports are the monitored ports. The state of a monitor link group adapts to that of its member uplink ports. When a monitor link group contains no uplink port or all the uplink ports are down, the monitor link group becomes down; as long as one member uplink port is up, the monitor link group stays up.
- Downlink ports are the monitoring ports. The state of the downlink ports in a monitor link group adapts to that of the monitor link group. The state of the downlink ports in a monitor link group is always consistent with that of the monitor link group.

Uplink/Downlink

The uplink is the link that connects the uplink ports in a monitor link group, and the downlink is the link that connects the downlink ports.

How Monitor Link works

Each monitor link group works independently of other monitor link groups. When a monitor link group contains no uplink port or all its uplink ports are down, the monitor link group goes down, which forces all its downlink ports down at the same time. When any uplink port goes up, the monitor link group goes up and brings up all its downlink ports.

CAUTION:

HP does not recommend to manually shut down or bring up the downlink ports in a monitor link group.

Configuring Monitor Link

Configuration prerequisites

Before assigning a port to a monitor link group, make sure the port is not the member port of any aggregation group.

Creating a monitor link group

Follow these steps to create a monitor link group:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a monitor link group and enter monitor link group view	**monitor-link group** *group-id*	Required

Configuring monitor link group member ports

You can configure member ports for a monitor link group in either monitor link group view or port view. Configurations made in these two views lead to the same result.

In monitor link group view

Follow these steps to configure member ports for a monitor link group in monitor link group view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter monitor link group view	**monitor-link group** *group-id*	—
Configure member ports for the monitor link group	**port** *interface-type interface-number* { **uplink** | **downlink** }	Required

In port view

Follow these steps to configure member ports for a monitor link group in port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view or Layer 2 aggregate port view	**interface** *interface-type interface-number*	—
Configure the current port as a member of a monitor link group	**port monitor-link group** *group-id* { **uplink** | **downlink** }	Required

NOTE:

- You can assign a Layer 2 Ethernet port or Layer 2 aggregate port to a monitor link group as a member port.
- A port can be assigned to only one monitor link group.
- Configure uplink ports prior to downlink ports to avoid undesired down/up state changes on the downlink ports.

Displaying and maintaining Monitor Link

To do…	Use the command…	Remarks
Display monitor link group information	**display monitor-link group** { *group-id* | **all** } [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Monitor Link configuration example

Network requirements

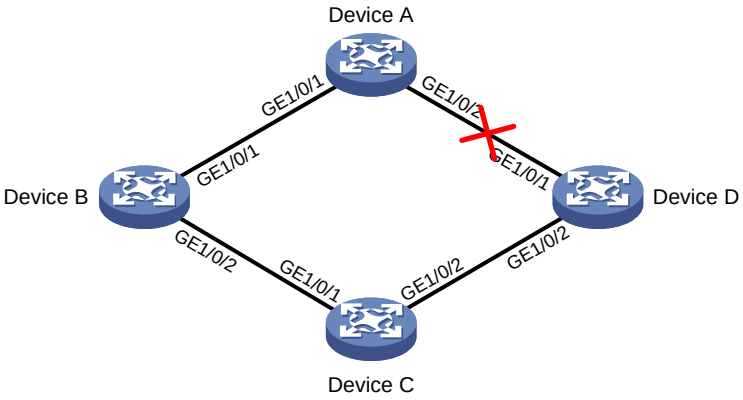
As shown in Figure 17:

- Device C is a smart link device, and Device A, Device B, and Device D are associated devices. Traffic of VLANs 1 through 30 on Device C is dual-uplinked to Device A through a smart link group.
- Implement dual uplink backup on Device C, and ensure that when the link between Device A and Device B (or Device D) fails, Device C can sense the link fault and perform uplink switchover in the smart link group.

NOTE:

For more information about Smart Link, see the chapter “Smart link configuration.”

Figure 17 Network diagram for monitor link configuration



Configuration procedure

1. Configuration on Device C

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

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

Disable STP on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 separately, configure them as trunk ports, and assign them to VLANs 1 through 30.

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

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

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

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

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

Enable the smart link group to transmit flush messages.

```
[DeviceC-smlk-group1] flush enable
[DeviceC-smlk-group1] quit
```

2. Configuration on Device A

Create VLANs 1 through 30.

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

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports, assign them to VLANs 1 through 30, and enable flush message receiving on them.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable
[DeviceA-GigabitEthernet1/0/2] quit
```

3. Configuration on Device B

Create VLANs 1 through 30.

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

Configure GigabitEthernet 1/0/1 as a trunk port assign it to VLANs 1 through 30, and enable flush message receiving on it.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port and assign it to VLANs 1 through 30. Disable the spanning tree feature and enable flush message receiving on it.

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

Create monitor link group 1, and then configure GigabitEthernet 1/0/1 as an uplink port and GigabitEthernet 1/0/2 as a downlink port for monitor link group 1.

```
[DeviceB] monitor-link group 1
[DeviceB-mtlk-group1] port gigabitethernet 1/0/1 uplink
[DeviceB-mtlk-group1] port gigabitethernet 1/0/2 downlink
[DeviceB-mtlk-group1] quit
```

4. Configuration on Device D

Create VLANs 1 through 30.

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

Configure GigabitEthernet 1/0/1 as a trunk port, assign it to VLANs 1 through 30, and enable flush message receiving on it.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable
[DeviceD-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port and assign it to VLANs 1 through 30. Disable the spanning tree feature and enable flush message receiving on it.

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

Create monitor link group 1, and then configure GigabitEthernet 1/0/1 as an uplink port and GigabitEthernet 1/0/2 as a downlink port for monitor link group 1.

```
[DeviceD] monitor-link group 1
[DeviceD-mtlk-group1] port gigabitethernet 1/0/1 uplink
[DeviceD-mtlk-group1] port gigabitethernet 1/0/2 downlink
[DeviceD-mtlk-group1] quit
```

5. Verify the configurations

Use the **display monitor-link group** command display the monitor link group information on devices. For example, when GigabitEthernet 1/0/2 on Device A goes down due to a link fault:

Check information about monitor link group 1 on Device B.

```
[DeviceB] display monitor-link group 1
 Monitor link group 1 information:
 Group status: UP
 Last-up-time: 16:37:20 2009/4/21
 Last-down-time: 16:35:26 2009/4/21
 Member                    Role     Status
 ----------------------------------------
 GigabitEthernet1/0/1      UPLINK   UP
 GigabitEthernet1/0/2      DOWNLINK UP
```

Check information about monitor link group 1 on Device D.

```
[DeviceD] display monitor-link group 1
 Monitor link group 1 information:
 Group status: DOWN
 Last-up-time: 16:35:27 2009/4/21
 Last-down-time: 16:37:19 2009/4/21
 Member                    Role     Status
 ----------------------------------------
 GigabitEthernet1/0/1      UPLINK   DOWN
 GigabitEthernet1/0/2      DOWNLINK DOWN
```

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/wwalerts

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP A-Series Acronyms*.

Websites

- HP.com http://www.hp.com
- HP Networking http://www.hp.com/go/networking
- HP manuals http://www.hp.com/support/manuals
- HP download drivers and software http://www.hp.com/support/downloads
- HP software depot http://www.software.hp.com
- HP Education http://www.hp.com/learn

Conventions

This section describes the conventions used in this documentation set.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk-marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x | y | ...] *	Asterisk-marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in bold text. For example, the **New User** window appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
TIP	An alert that provides helpful information.

Network topology icons

	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index

A C D E H M O R S T

A

Availability evaluation, 1
Availability requirements, 1

C

CFD configuration example, 28
CFD configuration task list, 19
Configuring a smart link device, 56
Configuring an associated device, 58
Configuring basic CFD settings, 20
Configuring basic Ethernet OAM functions, 8
Configuring CFD functions, 23
Configuring DLDP authentication, 44
Configuring link monitoring, 9
Configuring Monitor Link, 70
Configuring OAM remote loopback, 11
Configuring the Ethernet OAM connection detection timers, 9
Contacting HP, 75
Conventions, 76

D

Displaying and maintaining CFD, 27
Displaying and maintaining DLDP, 45
Displaying and maintaining Ethernet OAM configuration, 12
Displaying and maintaining Monitor Link, 71
Displaying and maintaining Smart Link, 59
DLDP configuration examples, 45
DLDP configuration task list, 41

E

Enabling DLDP, 41
Ethernet OAM configuration example, 12
Ethernet OAM configuration task list, 8
Ethernet OAM overview, 4

H

High availability technologies, 2

M

Monitor Link configuration example, 71

O

Overview (Monitor Link), 69
Overview (CFD), 15
Overview (DLDP), 34

R

Related information, 75
Resetting DLDP state, 44

S

Setting DLDP mode, 42
Setting the DelayDown timer, 43
Setting the interval for sending advertisement packets, 42
Setting the port shutdown mode, 43
Smart Link configuration examples, 59
Smart Link configuration task list, 56
Smart Link overview, 53

T

Troubleshooting DLDP, 52