



Quidway S5300 Series Ethernet Switches
V100R002C02

Configuration Guide - Availability

Issue	01
Date	2008-12-26
Part Number	

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. For any assistance, please contact our local office or company headquarters.

Huawei Technologies Co., Ltd.

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

Website: <http://www.huawei.com>

Email: support@huawei.com

Copyright © Huawei Technologies Co., Ltd. 2008. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

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

Notice

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

Contents

About This Document.....	1
1 Ethernet OAM Configuration.....	1-1
1.1 Introduction.....	1-2
1.1.1 Ethernet OAM Overview.....	1-2
1.1.2 Ethernet OAM Supported by the S-switch.....	1-2
1.2 Configuring EFM OAM.....	1-3
1.2.1 Establishing the Configuration Task.....	1-4
1.2.2 Enabling EFM OAM Globally.....	1-4
1.2.3 Configuring the Working Mode of EFM OAM on an Interface.....	1-5
1.2.4 (Optional) Setting the Maximum Size of an EFM OAMPDU.....	1-5
1.2.5 Enabling EFM OAM on an Interface.....	1-6
1.2.6 Checking the Configuration.....	1-6
1.3 Configuring EFM OAM Link Monitoring.....	1-7
1.3.1 Establishing the Configuration Task.....	1-7
1.3.2 (Optional) Detecting Errored Frames of EFM OAM.....	1-8
1.3.3 (Optional) Detecting Errored Codes of EFM OAM.....	1-8
1.3.4 (Optional) Detecting Errored Frame Seconds of EFM OAM.....	1-9
1.3.5 Checking the Configuration.....	1-10
1.4 Testing the Packet Loss Ratio on a Link.....	1-10
1.4.1 Establishing the Configuration Task.....	1-10
1.4.2 Configuring EFM OAM Remote Loopback.....	1-11
1.4.3 Sending Test Packets.....	1-12
1.4.4 Checking the Statistics on Returned Test Packets.....	1-12
1.4.5 (Optional) Manually Disabling EFM OAM Remote Loopback.....	1-13
1.4.6 Checking the Configuration.....	1-14
1.5 Associating EFM OAM with an Interface.....	1-14
1.5.1 Establishing the Configuration Task.....	1-14
1.5.2 Associating EFM OAM with an Interface.....	1-15
1.5.3 Checking the Configuration.....	1-15
1.6 Configuring Ethernet CFM.....	1-16
1.6.1 Establishing the Configuration Task.....	1-16
1.6.2 Enabling Ethernet CFM Globally.....	1-17
1.6.3 Creating an MD.....	1-18

1.6.4 Creating an MA.....	1-18
1.6.5 Creating a MEP.....	1-19
1.6.6 Creating an RMEP.....	1-20
1.6.7 (Optional) Setting the Rule for Creating a MIP.....	1-20
1.6.8 Enabling CC Detection.....	1-21
1.6.9 Checking the Configuration.....	1-22
1.7 Fault Verification on the Ethernet.....	1-24
1.7.1 Establishing the Configuration Task.....	1-24
1.7.2 (Optional) Implementing 802.1ag MAC Ping.....	1-25
1.7.3 (Optional) Implementing MAC Ping.....	1-25
1.8 Locating the Fault on the Ethernet.....	1-26
1.8.1 Establishing the Configuration Task.....	1-26
1.8.2 (Optional) Implementing 802.1ag MAC Trace.....	1-27
1.8.3 (Optional) Implementing MAC Trace.....	1-28
1.9 Maintaining Ethernet OAM.....	1-28
1.9.1 Clearing the Statistics on Error CCMs.....	1-28
1.9.2 Debugging EFM OAM.....	1-29
1.9.3 Monitoring the Running Status of Ethernet OAM.....	1-29
1.10 Configuration Examples.....	1-29
1.10.1 Example for Configuring EFM OAM.....	1-30
1.10.2 Example for Testing the Packet Loss Ratio on a Link.....	1-32
1.10.3 Example for Configuring Ethernet CFM.....	1-35
2 BFD Configuration.....	2-1
2.1 Introduction.....	2-2
2.1.1 BFD Overview.....	2-2
2.1.2 BFD Features Supported by the S-switch.....	2-2
2.1.3 Logical Relationships Between Configuration Tasks.....	2-3
2.1.4 Update History.....	2-3
2.2 Configuring the Single-Hop BFD.....	2-3
2.2.1 Establishing the Configuration Task.....	2-4
2.2.2 Enabling Global BFD.....	2-4
2.2.3 (Optional) Setting the Default Multicast IP Address.....	2-4
2.2.4 Creating a BFD Session.....	2-5
2.2.5 (Optional) Configuring Descriptions of the BFD Session.....	2-5
2.2.6 Checking the Configuration.....	2-6
2.3 Configuring the Multi-Hop BFD.....	2-7
2.3.1 Establishing the Configuration Task.....	2-8
2.3.2 Enabling Global BFD.....	2-8
2.3.3 Creating a BFD Session.....	2-8
2.3.4 (Optional) Configuring Descriptions of the BFD Session.....	2-9
2.3.5 Checking the Configuration.....	2-9
2.4 Associating the BFD Session Status with the Interface Status.....	2-11

2.4.1 Establishing the Configuration Task.....	2-11
2.4.2 Associating the BFD Session Status with the Interface Status.....	2-12
2.4.3 Checking the Configuration.....	2-12
2.5 Adjusting BFD Detection Parameters.....	2-14
2.5.1 Establishing the Configuration Task.....	2-14
2.5.2 Adjusting the BFD Detection Time.....	2-15
2.5.3 Setting the WTR for a BFD Session.....	2-16
2.5.4 Setting the Priority of BFD Packets.....	2-16
2.5.5 Checking the Configuration.....	2-17
2.6 Maintaining BFD.....	2-19
2.6.1 Clearing the BFD Statistics.....	2-20
2.6.2 Debugging BFD.....	2-20
2.7 Configuration Examples.....	2-20
2.7.1 Example for Configuring the Single-Hop BFD.....	2-20
2.7.2 Example for Configuring Multi-Hop BFD.....	2-23
3 Smart Link Configuration.....	3-1
3.1 Introduction.....	3-2
3.1.1 Smart Link and Monitor Link.....	3-2
3.1.2 Logical Relationships Between Configuration Tasks.....	3-2
3.2 Configuring Basic Functions of a Smart Link Group.....	3-2
3.2.1 Establishing the Configuration Task.....	3-3
3.2.2 Creating a Smart Link Group and Enabling Smart Link.....	3-4
3.2.3 Configuring the Master and Slave Interfaces of the Smart Link Group.....	3-4
3.2.4 (Optional) Enabling Revertive Switching of the Smart Link Group and Setting the WTR Time.....	3-5
3.2.5 (Optional) Enabling the Sending of Flush Packets.....	3-5
3.2.6 (Optional) Enabling the Receiving of Flush Packets.....	3-5
3.2.7 Checking the Configuration.....	3-6
3.3 Configuring the Data Stream Policy of the Smart Link Group.....	3-7
3.3.1 Establishing the Configuration Task.....	3-7
3.3.2 Locking Data Streams to the Master Interface.....	3-8
3.3.3 Locking Data Streams to the Slave Interface.....	3-8
3.3.4 Unlocking Data Streams.....	3-9
3.3.5 Configuring the Manual Switching of Data Streams.....	3-9
3.3.6 Checking the Configuration.....	3-9
3.4 Configuring Functions of a Monitor Link Group.....	3-10
3.4.1 Establishing the Configuration Task.....	3-10
3.4.2 Creating a Monitor Link Group.....	3-11
3.4.3 Configuring the Uplink and Downlink Interfaces of the Monitor Link Group.....	3-11
3.4.4 Configuring the WTR Time of the Monitor Link Group.....	3-12
3.4.5 Checking the Configuration.....	3-12
3.5 Maintaining Smart Link.....	3-13
3.6 Configuration Examples.....	3-13

3.6.1 Example for Configuring Basic Functions of Smart Link.....	3-13
3.6.2 Example for Configuring the Integrated Application of Smart Link.....	3-16

4 VRRP Configuration.....4-1

4.1 Introduction.....	4-2
4.1.1 VRRP Overview.....	4-2
4.1.2 VRRP Features Supported by the S-switch.....	4-2
4.2 Configuring a VRRP Backup Group.....	4-3
4.2.1 Establishing the Configuration Task.....	4-4
4.2.2 Creating a Backup Group and Configuring the Virtual IP Address.....	4-5
4.2.3 Configuring the Priority of an Interface in a Backup Group.....	4-5
4.2.4 Checking the Configuration.....	4-6
4.3 Configuring VRRP to Track the Status of an Interface.....	4-7
4.3.1 Establishing the Configuration Task.....	4-7
4.3.2 Configuring VRRP to Track the Status of an Interface.....	4-8
4.3.3 Checking the Configuration.....	4-8
4.4 Configuring VRRP Fast Switchover.....	4-9
4.4.1 Establishing the Configuration Task.....	4-9
4.4.2 Tracking the BFD Session Status.....	4-10
4.4.3 Checking the Configuration.....	4-10
4.5 Configuring VRRP on VLANIF Interfaces.....	4-11
4.5.1 Establishing the Configuration Task.....	4-11
4.5.2 Configuring VRRP on VLANIF Interfaces.....	4-11
4.5.3 (Optional) Setting the Sending Mode of VRRP Packets in the Super-VLAN.....	4-12
4.5.4 Checking the Configuration.....	4-12
4.6 Configuring the VRRP Security Function.....	4-13
4.6.1 Establishing the Configuration Task.....	4-13
4.6.2 Setting the Authentication Mode for VRRP Packets.....	4-14
4.6.3 Checking the Configuration.....	4-14
4.7 Adjusting and Optimizing VRRP.....	4-15
4.7.1 Establishing the Configuration Task.....	4-15
4.7.2 Configuring the Interval for Sending VRRP Advertisement Packets.....	4-16
4.7.3 Configuring the Preemption Delay for the S-switches in the Backup Group.....	4-16
4.7.4 Ping to the Virtual IP Address.....	4-17
4.7.5 Disabling the Detection of the TTL Value of VRRP Packets.....	4-18
4.7.6 Configuring the Timeout Period for the Master S-switch to Send Gratuitous ARP Packets.....	4-18
4.7.7 Configuring the VRRP NMS.....	4-19
4.7.8 Checking the Configuration.....	4-19
4.8 Maintaining VRRP.....	4-20
4.8.1 Monitoring the VRRP Running Status.....	4-20
4.8.2 Debugging VRRP.....	4-20
4.9 Configuration Examples.....	4-20
4.9.1 Example for Combining NAT and VRRP.....	4-21

4.9.2 Example for Configuring VRRP in Master/Backup Mode.....4-25

4.9.3 Example for Configuring VRRP in Load Balancing Mode.....4-29

Figures

Figure 1-1 Networking for configuring EFM OAM.....	1-4
Figure 1-2 Networking for testing the packet loss ratio on a link.....	1-11
Figure 1-3 Networking for associating EFM OAM with an interface.....	1-15
Figure 1-4 Networking for configuring EFM OAM.....	1-30
Figure 1-5 Networking for testing the packet loss ratio on a link.....	1-33
Figure 1-6 Diagram of configuring Ethernet CFM.....	1-36
Figure 2-1 Networking diagram of configuring the single-hop BFD for Layer 2 forwarding link.....	2-21
Figure 2-2 Networking diagram of configuring the multi-hop BFD.....	2-23
Figure 3-1 Applicable environment of Smart Link.....	3-3
Figure 3-2 Configuring the data stream policy.....	3-7
Figure 3-3 Applicable environment of Monitor Link.....	3-10
Figure 3-4 Example for configuring basic functions of Smart Link.....	3-14
Figure 3-5 Example for configuring the integrated application of Smart Link.....	3-17
Figure 4-1 Default gateway in a LAN.....	4-2
Figure 4-2 Networking diagram of combining NAT and VRRP.....	4-21
Figure 4-3 Networking diagram of configuring VRRP in master/backup mode.....	4-26
Figure 4-4 Networking diagram of configuring VRRP in load balancing mode.....	4-30

About This Document

Purpose

This document describes procedures and provides examples for configuring the availability features of the S-switch.

This document covers the following topics:

- Feature description
- Data preparation
- Pre-configuration tasks
- Configuration procedures
- Checking the configuration
- Configuration examples

This document guides you through the configuration and applicable environment of the availability features of the S-switch.

Related Versions

The following table lists the product versions related to this document.

Product Name	Version
S5300	V100R002C02

Intended Audience

This document is intended for:

- Commissioning engineers
- Data configuration engineers
- Network monitoring engineers
- System maintenance engineers

Organization






This document is organized as follows.

Chapter	Description
1 Ethernet OAM Configuration	This chapter describes the basics and configuration of OAM.
2 BFD Configuration	This chapter describes the basic principle of BFD, configurations of basic functions, and provides configuration examples.
3 Smart Link Configuration	This chapter describes the implementation and configuration procedures of Smart Link on the S-switch.
4 VRRP Configuration	This chapter describes the principle of the Virtual Router Redundancy Protocol (VRRP), commands for maintaining VRRP, and the configurations of basic and advanced functions of VRRP as well as configuration examples.

Conventions

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
 WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injuries.
 CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 TIP	Indicates a tip that may help you address a problem or save your time.
 NOTE	Provides additional information to emphasize or supplement important points of the main text.

General Conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Boldface	Names of files, directories, folders, and users are in boldface . For example, log in as user root .
<i>Italic</i>	Book titles are in italics.
Courier New	Terminal display is in Courier New. The messages input on terminals by users that are displayed are in boldface.

Command Conventions

Convention	Description
Boldface	The keywords of a command line are in boldface .
<i>Italic</i>	Command arguments are in <i>italics</i> .
[]	Items (keywords or arguments) in brackets [] are optional.
{ x y ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x y ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x y ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x y ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

GUI Conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in boldface . For example, click OK .
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose File > Create > Folder .

Keyboard Operations

Format	Description
Key	Press the key. For example, press Enter and press Tab .
Key 1+Key 2	Press the keys concurrently. For example, pressing Ctrl+Alt+A means the three keys should be pressed concurrently.
Key 1, Key 2	Press the keys in turn. For example, pressing Alt, A means the two keys should be pressed in turn.

Mouse Operation

Action	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

Update History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Updates in Issue 01 (2008-12-26)

This is the first release.

1 Ethernet OAM Configuration

About This Chapter

[1.1 Introduction](#)

This section describes the background and functions of Ethernet Operation, Administration, and Maintenance (OAM), and the Ethernet OAM functions supported by the S-switch.

[1.2 Configuring EFM OAM](#)

[1.3 Configuring EFM OAM Link Monitoring](#)

[1.4 Testing the Packet Loss Ratio on a Link](#)

This section describes the method of testing the packet loss ratio on a link by configuring remote loopback and sending testing packets.

[1.5 Associating EFM OAM with an Interface](#)

[1.6 Configuring Ethernet CFM](#)

This section describes how to configure Ethernet CFM.

[1.7 Fault Verification on the Ethernet](#)

This section describes the method of testing the connectivity on the Ethernet through 802.1ag MAC ping or MAC ping.

[1.8 Locating the Fault on the Ethernet](#)

This section describes the method of locating the connectivity fault on the Ethernet through 802.1ag MAC trace or MAC trace.

[1.9 Maintaining Ethernet OAM](#)

This section describes how to debug EFM OAM, how to monitor the running status of Ethernet OAM, and how to clear the statistics on error CCMs.

[1.10 Configuration Examples](#)

This section provides several configuration examples of Ethernet OAM.

1.1 Introduction

This section describes the background and functions of Ethernet Operation, Administration, and Maintenance (OAM), and the Ethernet OAM functions supported by the S-switch.

1.1.1 Ethernet OAM Overview

1.1.2 Ethernet OAM Supported by the S-switch

1.1.1 Ethernet OAM Overview

Background

The Ethernet has developed as the major Local Area Network (LAN) technology because it features easy implementation and low cost. Recently, along with the applications of the Gigabit Ethernet (GE) and the later 10 Gigabit Ethernet (10GE), the Ethernet has been extended to the Metropolitan Area Network (MAN) and Wide Area Network (WAN).

Compared with MANs and WANs, reliability and stability are not highly required for LANs. Therefore, a mechanism for network OAM is always required for the Ethernet. The lack of the OAM mechanism prevents the Ethernet from effectively functioning as the Internet Service Provider (ISP) network. In this manner, Ethernet OAM is becoming a trend.

Functions

Ethernet OAM has the following functions:

- Fault management
Ethernet OAM can detect the network connectivity by sending detection messages regularly or through manual triggering.
- Performance management
Performance management is used to measure the packet loss ratio, delay, and jitter during the transmission of packets. It also collects statistics on various types of traffic. Performance management is implemented at the access point of users. By using the performance management tools, the ISP can monitor the network status and locate faults through the Network Management System (NMS). The ISP checks whether the forwarding capability of the network complies with the Service Level Agreement (SLA) signed with users.

Ethernet OAM improves network management and maintenance capabilities on the Ethernet and guarantees a steady network.

1.1.2 Ethernet OAM Supported by the S-switch

EFM OAM

EFM OAM supported by the S-switch provides the following functions:

- OAM discovery
When an interface on the S-switch and the peer are both enabled with Ethernet in the First Mile (EFM) OAM, the interface and the peer send and respond with an OAM Protocol Data

Unit (OAMPDU) to determine whether the EFM OAM configurations on both interfaces match. This is called OAM discovery. If the EFM OAM configurations on both interfaces match, the two interfaces enter the EFM OAM Detect state. In the Detect state, the two interfaces send OAMPDUs regularly to maintain adjacencies.

- Link monitoring

Link monitoring is a mechanism for an interface to notify the peer of the fault by sending the event notification OAMPDU when the interface detects the errored frame event, errored code event, or errored frame seconds event.

- The errored frame event means that the number of errored frames detected on an interface reaches or exceeds a specified threshold within a set period.
- The errored code event means that the number of errored codes detected on an interface reaches or exceeds a specified threshold within a set period.
- The errored frame seconds summary event means that the number of errored frame seconds detected on an interface reaches or exceeds a specified threshold within a set period.

An errored frame second is a one-second interval during which at least one errored frame is detected

- Fault notification

When a link event about a fault occurs on a local interface, the local interface notifies the peer of the fault through OAMPDUs. The local interface then records the event in the log, and reports it to the NMS. This is called fault notification.

- The system reboots.
- A physical link fails.
- OAMPDUs time out.

After receiving OAMPDUs, the peer records the event carried in OAMPDUs to the log, and reports it to the NMS.

- Remote loopback

When a local interface sends non-OAMPDUs to the peer, instead of forwarding non-OAMPDUs based on their destination MAC addresses, the peer loops back non-OAMPDUs to the local interface. This is called remote loopback. Remote loopback can be used to locate faults and test link performance.

The working mode of EFM OAM is an attribute of the interface enabled with EFM OAM. The working mode of EFM OAM on an interface is either active or passive. OAM discovery and remote loopback are initiated only by the interface in active mode.

Fault Association

- Association between EFM OAM and an interface

When an interface enabled with EFM OAM detects a connectivity fault between the interface and the peer, the OAM management module performs the restart function, that is, shuts down the interface for 3 seconds and then turns it on so that the other modules can sense the fault.

1.2 Configuring EFM OAM

1.2.1 Establishing the Configuration Task

[1.2.2 Enabling EFM OAM Globally](#)[1.2.3 Configuring the Working Mode of EFM OAM on an Interface](#)[1.2.4 \(Optional\) Setting the Maximum Size of an EFM OAMPDU](#)[1.2.5 Enabling EFM OAM on an Interface](#)[1.2.6 Checking the Configuration](#)

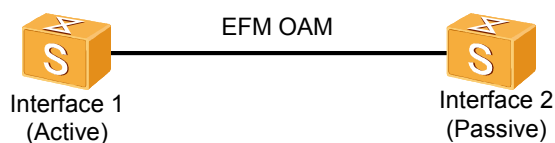
1.2.1 Establishing the Configuration Task

Applicable Environment

As shown in [Figure 1-1](#), you can perform the configuration task to implement the following functions:

- Detecting the connectivity between two directly connected devices
- Implementing fault notification between two directly connected devices
- After receiving OAMPDUs, the peer records the event carried in OAMPDUs to the log, and reports it to the NMS.

Figure 1-1 Networking for configuring EFM OAM



The interface view mentioned in this section refers to the view of the interface on the link to be tested, such as the view of interface 1 or interface 2 in [Figure 1-1](#).

Pre-configuration Tasks

None.

Data Preparation

To configure EFM OAM, you need the following data.

No.	Data
1	(Optional) Maximum size of an EFM OAMPDU

1.2.2 Enabling EFM OAM Globally

Context

Do as follows on the devices at both ends of the link.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **efm enable** command to enable EFM OAM globally.

By default, EFM OAM is disabled globally.

----End

1.2.3 Configuring the Working Mode of EFM OAM on an Interface

Context

Do as follows on the devices at both ends of the link.

NOTE

The working mode of EFM OAM on an interface can be configured only after EFM OAM is enabled globally and before EFM OAM is enabled on the interface. The working mode of EFM OAM on an interface cannot be modified after EFM OAM is enabled on the interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **efm mode { active | passive }** command to configure the working mode of EFM OAM on the interface.

By default, EFM OAM on an interface works in active mode.

At least one interface at both ends of the link must be configured to work in active mode. The interface in active mode initiates OAM discovery after EFM OAM is enabled on the interface. Instead of initiating OAM discovery, the interface in passive mode waits for an OAMPDU sent from the interface in active mode. If both interfaces are configured to work in passive mode, OAM discovery fails.

----End

1.2.4 (Optional) Setting the Maximum Size of an EFM OAMPDU

Context

Do as follows on the devices at both ends of the link.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **efm packet max-size** *size* command to set the maximum size of an EFM OAMPDU.

By default, the maximum size of an EFM OAMPDU on an interface is 128 bytes.

EFM OAMPDUs that exceed 128 bytes are discarded as invalid packets.

If the maximum size of an EFM OAMPDU on both interfaces of the link is configured differently, the two interfaces negotiate and determine the value during the OAM discovery process. The smaller maximum size of an EFM OAM PDU set on the local interface and the peer is selected.

----End

1.2.5 Enabling EFM OAM on an Interface

Context

Do as follows on the devices at both ends of the link.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface interface-type interface-number** command to enter the interface view.

Step 3 Run the **efm enable** command to enable EFM OAM on the interface.

By default, EFM OAM is disabled on an interface.

Step 4 Run the **bpdu enable** command to enable the interface to process Bridge Protocol Data Units (BPDUs).

NOTE

When using the **efm enable** command to enable EFM OAM on an interface, you need to use the **bpdu enable** command to allow BPDUs to pass through the interface. Otherwise, EFM OAMPDUs are discarded.

----End

1.2.6 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the EFM OAM configuration on an interface.	display efm { all interface interface-type interface-number }
Check the status of the EFM OAM protocol on an interface.	display efm session { all interface interface-type interface-number }

Run the **display efm** command. If all the EFM OAM configurations on the local interface and part of the EFM OAM configurations on the peer are displayed, it means that the configuration succeeds.

```
<Quidway> display efm interface gigabitethernet0/0/1
  Item                               Value
-----
Interface                           : GigabitEthernet0/0/1
EFM Enable Flag                      : enable
```

```

Mode : active
OAMPDU MaxSize : 128
ErrCodeNotification : disable
ErrCodePeriod : 1
ErrCodeThreshold : 1
ErrFrameNotification : disable
ErrFramePeriod : 1
ErrFrameThreshold : 1
ErrFrameSecondNotification : disable
ErrFrameSecondPeriod : 60
ErrFrameSecondThreshold : 1
TriggerIfDown : disable
Remote MAC : 0018-8200-0001
Remote EFM Enable Flag : enable
Remote Mode : passive
Remote MaxSize : 128

```

Run the **display efm session** command. If the EFM OAM protocol on the interface is in the Detect state, it means that the configuration succeeds. The two interfaces succeed in negotiation and enter the Detect state.

```

<Quidway> display efm session interface gigabitethernet0/0/1
Interface          EFM State          Loopback Timeout
-----
GigabitEthernet0/0/1  detect             --

```

1.3 Configuring EFM OAM Link Monitoring

1.3.1 Establishing the Configuration Task

1.3.2 (Optional) Detecting Errored Frames of EFM OAM

1.3.3 (Optional) Detecting Errored Codes of EFM OAM

1.3.4 (Optional) Detecting Errored Frame Seconds of EFM OAM

1.3.5 Checking the Configuration

1.3.1 Establishing the Configuration Task

Applicable Environment

You can perform the configuration task to monitor the errored frames, errored codes, and errored frame seconds on a link.



NOTE

The interface view mentioned in this section refers to the view of the interface attached to the link to be tested.

Pre-configuration Tasks

Before configuring EFM OAM link monitoring, complete the following task:

- [1.2 Configuring EFM OAM](#)

Data Preparation

To configure EFM OAM link monitoring, you need the following data.

No.	Data
1	(Optional) Period and threshold for detecting errored frames of EFM OAM
2	(Optional) Period and threshold for detecting errored codes of EFM OAM
3	(Optional) Period and threshold for detecting errored frame seconds of EFM OAM

1.3.2 (Optional) Detecting Errored Frames of EFM OAM

Context

Do as follows on the devices at one end or both ends of the link.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **efm error-frame period** *period* command to set the period for detecting errored frames on the interface.

By default, the period for detecting errored frames on an interface is 1 second.

Step 4 Run the **efm error-frame threshold** *threshold* command to set the threshold for detecting errored frames on the interface.

By default, the threshold for detecting errored frames on an interface is 1.

Step 5 Run the **efm error-frame notification enable** command to enable the interface to detect errored frames.

By default, an interface cannot detect errored frames.

----End

Postrequisite

When an interface is enabled to detect errored frames, the S-switch generates an errored frame event and notifies the peer, if the number of errored frames reaches or exceeds the threshold within a set period. The peer sends traps if the trap function is enabled on the peer.

1.3.3 (Optional) Detecting Errored Codes of EFM OAM

Context

Do as follows on the devices at one end or both ends of the link.

Procedure

Step 1 Run the **system-view** command to enter the system view.

- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **efm error-code period** *period* command to set the period for detecting errored codes on the interface.
- By default, the period for detecting errored codes on an interface is 1 second.
- Step 4** Run the **efm error-code threshold** *threshold* command to set the threshold for detecting errored codes on the interface.
- By default, the threshold for detecting errored codes on an interface is 1.
- Step 5** Run the **efm error-code notification enable** command to enable the interface to detect errored codes.
- By default, an interface cannot detect errored codes.
- End

Postrequisite

When an interface is enabled to detect errored codes, the S-switch generates an errored code event and notifies the peer, if the number of errored codes reaches or exceeds the threshold within a set period. The peer sends traps if the trap function is enabled on the peer.

1.3.4 (Optional) Detecting Errored Frame Seconds of EFM OAM

Context

Do as follows on the devices at one end or both ends of the link.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **efm error-frame-second period** *period* command to set the period for detecting errored frame seconds on the interface.
- By default, the period for detecting errored frame seconds on an interface is 60 seconds.
- Step 4** Run the **efm error-frame-second threshold** *threshold* command to set the threshold for detecting errored frame seconds on the interface.
- By default, the threshold for detecting errored frame seconds on an interface is 1.
- Step 5** Run the **efm error-frame-second notification enable** command to enable the interface to detect errored frame seconds.
- By default, an interface cannot detect errored frame seconds.
- End

Postrequisite

When an interface is enabled to detect errored frame seconds, the S-switch generates an errored frame seconds summary event and notifies the peer, if the number of errored frame seconds

reaches or exceeds the threshold within a set period. The peer sends traps if the trap function is enabled on the peer.

1.3.5 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the EFM OAM configuration on an interface.	display efm { all interface <i>interface-type interface-number</i> }

Run the **display efm** command. You can view information about link monitoring on an interface.

```
<Quidway> display efm interface gigabitethernet0/0/1
      Item                               Value
-----
Interface:                             GigabitEthernet0/0/1
EFM Enable Flag                         enable
Mode:                                   active
OAMPDU MaxSize:                         128
ErrCodeNotification:                   enable
ErrCodePeriod:                         1
ErrCodeThreshold:                      1
ErrFrameNotification:                  enable
ErrFramePeriod:                        1
ErrFrameThreshold:                    1
ErrFrameSecondNotification:            enable
ErrFrameSecondPeriod:                  60
ErrFrameSecondThreshold:              1
TriggerIfDown:                         disable
RemoteMAC                              0018-8200-0001
Remote EFM Enable Flag                 enable
Remote Mode                            passive
Remote MaxSize                         128
```

1.4 Testing the Packet Loss Ratio on a Link

This section describes the method of testing the packet loss ratio on a link by configuring remote loopback and sending testing packets.

1.4.1 Establishing the Configuration Task

1.4.2 Configuring EFM OAM Remote Loopback

1.4.3 Sending Test Packets

1.4.4 Checking the Statistics on Returned Test Packets

1.4.5 (Optional) Manually Disabling EFM OAM Remote Loopback

1.4.6 Checking the Configuration

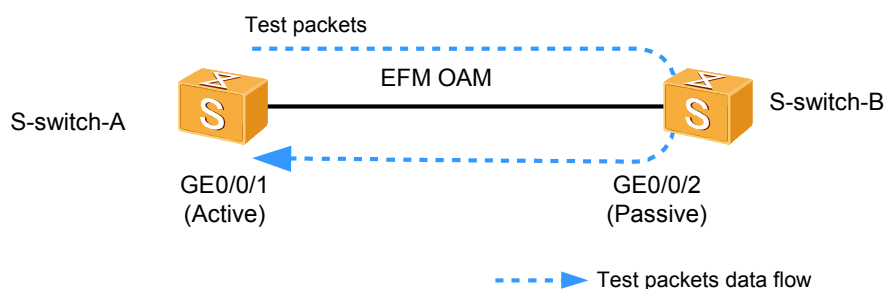
1.4.1 Establishing the Configuration Task

Applicable Environment

You can perform the configuration task to detect the packet loss ratio on a link.

As shown in **Figure 1-2**, configure EFM OAM on S-switch-A and S-switch-B, and configure remote loopback on GE 0/0/1 of S-switch-A. Send test packets from S-switch-A to S-switch-B. You can obtain the packet loss ratio on the link by checking the statistics on received test packets on S-switch-A.

Figure 1-2 Networking for testing the packet loss ratio on a link



NOTE

The interface view mentioned in this section refers to the view of the interface on the link to be tested.

Pre-configuration Tasks

Before testing the packet loss ratio on a link, complete the following task:

- **1.2 Configuring EFM OAM**

Data Preparation

To test the packet loss ratio on a link, you need the following data.

No.	Data
1	Timeout period for remote loopback
2	Destination MAC address, outbound interface, size, number, and VLAN ID of test packets

1.4.2 Configuring EFM OAM Remote Loopback

Context

Do as follows on the device with an active interface on the link.



CAUTION

The forwarding of service data is affected after EFM OAM remote loopback is enabled. So, enable EFM OAM remote loopback on the link that need not forward service data.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **efm loopback start [timeout timeout]** command to configure the interface to initiate remote loopback.

By default, the timeout period for remote loopback is 20 minutes. After 20 minutes, remote loopback stops. You can set the timeout period to 0 for a link to remain in the remote loopback state.

The following requirements must be met to implement remote loopback:

- The EFM OAM protocols on the local interface and the peer are in the Detect state.
- EFM OAM on the local interface works in active mode.

You can use the **display efm session** command to check whether the EFM OAM protocols running on the local interface and the peer are in the Detect state.

----End

1.4.3 Sending Test Packets

Context

Do as follows on the device with an active interface on the link.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **test-packet start [mac mac-address] [vlan vlan-id] interface interface-type interface-number [-c count | -s size] *** command to send test packets.

By default, the destination MAC address of the test packets is 00e0-fc00-0000; the size of a test packet is 64 bytes; the number of test packets being sent is 5. If the VLAN ID is not specified, test packets are sent without VLAN tags.

NOTE

The outbound interface for the test packets is the interface that connects the link to be tested. The destination MAC address of the test packets cannot be 000f-e207-8217 when EFM OAM remote loopback is configured on the Rapid Ring Protection Protocol (RRPP) links.

When the test packets reach the peer, the peer sends them back to the local device, irrespective of the destination MAC address of the test packets. As a result, **mac mac-address** is not required or you can set a random value for this parameter.

The parameters in this command cannot be modified when test packets are being sent. Press **Ctrl+C** to stop sending test packets. A device sends test packets once at a time.

----End

1.4.4 Checking the Statistics on Returned Test Packets

Context

Do as follows on the device with an active interface on the link.

Procedure

Run the **display test-packet result** command to view the statistics on returned test packets.

```
<Quidway> display test-packet result
Test Item                               Test Result
-----
PacketsSend:                           5  PacketsReceive:                    5
PacketsLost:                           0  BytesSend:                      320
BytesReceive:                          320 BytesLost:                    0
StartTime:                             10:12:2008-16:09:48 EndTime:
10:12:2008-16:09:49
```

The displayed information includes:

- Number of sent test packets
- Number of received test packets
- Number of discarded test packets
- Total number of bytes of sent test packets
- Total number of bytes of received test packet
- Total number of bytes of discarded test packet
- Time to start sending test packets
- Time to stop sending test packets

You can obtain the packet loss ratio on the link based on the preceding data.

----End

1.4.5 (Optional) Manually Disabling EFM OAM Remote Loopback

Context

Do as follows on the device with an active interface on the link.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **efm loopback stop** command to disable EFM OAM remote loopback on the interface.

If EFM OAM remote loopback is left enabled, the link fails to forward service data for a long time. To avoid this, EFM OAM remote loopback on the S-switch can be automatically disabled after a timeout period. By default, the timeout period for remote loopback is 20 minutes. After 20 minutes, remote loopback stops.

If you need to disable remote loopback manually, perform the preceding procedures.

----End

1.4.6 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the status of the EFM OAM protocol on an interface.	display efm session { all interface <i>interface-type interface-number</i> }

Run the **display efm session** command on the device with an active interface on the link. If the EFM OAM protocol on the active interface is in the Loopback (control) state, which indicates that the active interface initiates remote loopback, it means that the configuration succeeds.

```
<S-switch-A> display efm session interface gigabitethernet 0/0/1
Interface           EFM State           Loopback Timeout
-----
GigabitEthernet0/0/1  loopback (control)   20
```

Run the **display efm session** command on the device with a passive interface on the link. If the EFM OAM protocol on the passive interface is in the Loopback (be controlled) state, which indicates that the passive interface responds to remote loopback, it means that the configuration succeeds.

```
<S-switch-B> display efm session interface gigabitethernet 0/0/2
Interface           EFM State           Loopback Timeout
-----
GigabitEthernet0/0/2  loopback (be controlled)  --
```

Run the **display efm session** command on either of the two devices on the link after remote loopback is automatically or manually disabled, you can view that the status of the EFM OAM protocol on the interface is no longer Loopback (control) or Loopback (be controlled).

```
<S-switch-A> display efm session interface gigabitethernet 0/0/1
Interface           EFM State           Loopback Timeout
-----
GigabitEthernet0/0/1  detect              --
```

1.5 Associating EFM OAM with an Interface

1.5.1 Establishing the Configuration Task

1.5.2 Associating EFM OAM with an Interface

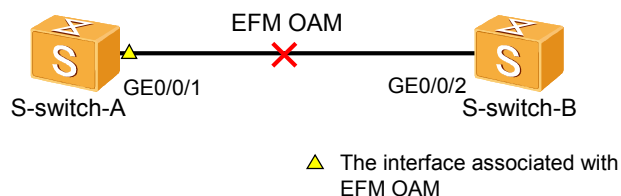
1.5.3 Checking the Configuration

1.5.1 Establishing the Configuration Task

Applicable Environment

As shown in [Figure 1-3](#), EFM OAM is enabled on S-switch-A and S-switch-B. EFM OAM is associated with GE 0/0/1 on S-switch-A. When the EFM OAM module on S-switch-A detects a connectivity fault between S-switch-A and S-switch-B, the OAM management module shuts down and then starts GE 0/0/1 after 3 seconds so that the other modules can sense the fault.

Figure 1-3 Networking for associating EFM OAM with an interface



NOTE

The interface view mentioned in this section refers to the view of the interface on the link to be tested.

Pre-configuration Tasks

Before associating EFM OAM with an interface, complete the following task:

- [1.2 Configuring EFM OAM](#)

Data Preparation

To associate EFM OAM with an interface, you need the following data.

No.	Data
1	Type and number of an interface

1.5.2 Associating EFM OAM with an Interface

Context

Do as follows on the devices at one end or both ends of the link.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **efm trigger if-down** command to associate EFM OAM with the interface.

By default, EFM OAM is not associated with interfaces.

The **efm trigger if-down** command is valid in the interface view only after EFM OAM is enabled on the interface with the **efm enable** command.

----End

1.5.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the EFM OAM configuration on an interface.	display efm { all interface <i>interface-type interface-number</i> }

Run the **display efm** command. If the item "TriggerIfDown" is displayed as **enable**, it means that the configuration succeeds.

```
<Quidway> display efm interface gigabitethernet0/0/1
  Item                               Value
-----
Interface:                          GigabitEthernet0/0/1
EFM Enable Flag:                     enable
Mode:                                active
OAMPDU MaxSize:                      128
ErrCodeNotification:                 disable
ErrCodePeriod:                       1
ErrCodeThreshold:                    1
ErrFrameNotification:                 disable
ErrFramePeriod:                      1
ErrFrameThreshold:                   1
ErrFrameSecondNotification:           disable
ErrFrameSecondPeriod:                 60
ErrFrameSecondThreshold:              1
TriggerIfDown:                       enable
Remote MAC:                          0018-8200-0001
Remote EFM Enable Flag:               enable
Remote Mode:                          passive
Remote MaxSize:                       128
```

1.6 Configuring Ethernet CFM

This section describes how to configure Ethernet CFM.

[1.6.1 Establishing the Configuration Task](#)

[1.6.2 Enabling Ethernet CFM Globally](#)

[1.6.3 Creating an MD](#)

[1.6.4 Creating an MA](#)

[1.6.5 Creating a MEP](#)

[1.6.6 Creating an RMEP](#)

[1.6.7 \(Optional\) Setting the Rule for Creating a MIP](#)

[1.6.8 Enabling CC Detection](#)

[1.6.9 Checking the Configuration](#)

1.6.1 Establishing the Configuration Task

Applicable Environment

You can perform the configuration task to implement the following functions on the Ethernet:

- Automatic end-to-end connectivity detection
- Automatic connectivity detection on directly connected links

You need to ensure that the following conditions be met before implementing automatic end-to-end connectivity detection on the Ethernet:

- MDs are classified based on the ISP that manages the devices. All the devices that are managed by a single ISP and enabled with CFM can be configured in an MD.
- MAs are classified based on different SIs. An MA is associated with a VLAN. A VLAN generally maps to an SI. When the MA is classified, fault detection in connectivity can be carried out on the network where an SI is transmitted.
- You need to determine the interfaces on which devices are located at the edge of the MA, that is, to determine that MEPs must be configured on the interfaces on which devices.

When implementing automatic connectivity detection on directly connected links, you also need to ensure that:

- The devices at both ends must be configured in the same MA within an MD.
- MEPs must be configured on the interfaces at both ends of the directly connected link.

Pre-configuration Tasks

None.

Data Preparation

To configure Ethernet CFM, you need the following data.

No.	Data
1	Name and level of an MD
2	Name of an MA, ID of the VLAN associated with the MA
3	ID of a MEP, name of the interface on which the MEP resides, type of the MEP
4	ID of an RMEP and (Optional) bridge MAC address of the device on which the RMEP resides
5	Rule for creating a MIP
6	Interval for a MEP sending or detecting CCMs in an MA

1.6.2 Enabling Ethernet CFM Globally

Context

Do as follows on the S-switch that requires Ethernet CFM:

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **cfm enable** command to enable Ethernet CFM globally.
- By default, Ethernet CFM on the S-switch is disabled globally.

----End

1.6.3 Creating an MD

Context

Do as follows on the S-switch that requires Ethernet CFM:

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **cfm md md-name [level level]** command to create an MD and enter the MD view.
- By default, an MD is at level 0. Level 0 is the lowest level.
- Repeat Step 2 to create more MDs. Up to 16 MDs can be created on the S-switch.



NOTE

The 802.1ag packets from a low-level MD are discarded in a high-level MD. The 802.1ag packets from a high-level MD can be transmitted through a low-level MD. The 802.1ag packets from an MD are not forwarded. Instead, they are processed according to the contents carried in the 802.1ag packets.

----End

1.6.4 Creating an MA

Context

Do as follows on the S-switch that requires Ethernet CFM:

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **cfm md md-name** command to enter the MD view.
- Step 3** Run the **ma ma-name** command to create an MA and enter the MA view.
- Up to 256 MAs can be created in an MD. On the S-switch, up to 256 MAs can be created.
- Step 4** Run the **map vlan vlan-id** command to associate the MA with a VLAN.

By default, an MA is not associated with any VLAN.

Ethernet CFM maintains the connectivity of each MA separately. After an MA is associated with a VLAN, Ethernet CFM can detect the connectivity fault on the network within the VLAN.

----End

Postrequisite

An MA is associated with a VLAN only.

- If you need to create multiple MAs in an MD, repeat [Step 3](#) and [Step 4](#).
- If you need to create multiple MAs in multiple MDs, repeat [Step 2](#) to [Step 4](#).

1.6.5 Creating a MEP

Context

When creating a MEP in an MA, also note that:

- When an inward-facing MEP is created, the MA must be associated with a VLAN and the interface on which the MEP resides must be added to the VLAN. The inward-facing MEP then broadcasts the OAMPDUs in the VLAN associated with the MA. That is, the inward-facing MEP sends the OAMPDUs out through all the interfaces excluding the interface on which the MEP resides in the VLAN associated with the MAC.
- When the outward-facing MEP is created, the MA must be associated with a VLAN and the interface on which the MEP resides must be added to the VLAN. The outward-facing MEP sends out the OAMPDUs through the interface on which the MEP resides.

The following lists the requirements for the number and types of MEPs created in an MA:

- The inward-facing interface-based MEP and the outward-facing interface-based MEP cannot coexist.
- Only one outward-facing interface-based MEP can be created. Multiple inward-facing interface-based MEPs can be created. However, only one inward-facing interface-based MEP can be created on an interface.

The number of MEPs that can be created in an MA is determined by the interval for a MEP sending or detecting CCMs in the MA. When the interval is 10s, you can create 256 MEPs; when the interval is 1s, you can create 32 MEPs; when the interval is 100 ms, you can create 2 MEPs.

Do as follows on the edge devices of an MA.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **cfm md md-name** command to enter the MD view.
- Step 3** Run the **ma ma-name** command to enter the MA view.
- Step 4** Run the **mep mep-id mep-id interface { interface-type interface-number } { inward | outward }** command to create an interface-based MEP.

----End

Postrequisite

On the S-switch, up to 8K MEPs can be created on each board, up to 16K MEPs can be created on the NE40E. up to 32K MEPs can be created on the NE80E.

- If you need to create multiple MEPs in an MA, repeat [Step 4](#).

- If you need to create multiple MEPs in multiple MAs, repeat [Step 3](#) and [Step 4](#).
- If you need to create multiple MEPs in multiple MDs, repeat [Step 2](#) to [Step 4](#).

1.6.6 Creating an RMEP

Context

If you need to detect the connectivity between a device and an RMEP, you need to create the RMEP first.

Do as follows on the edge devices of an MA:

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **cfm md md-name** command to enter the MD view.
- Step 3** Run the command to enter the MA view.
- Step 4** Run the **remote-mep mep-id mep-id [mac mac-address]** command to create an RMEP in the current MA.

----End

Postrequisite

- If you need to create multiple RMEPs in an MA, repeat [Step 4](#).
- If you need to create multiple RMEPs in multiple MAs, repeat [Step 3](#) and [Step 4](#).
- If you need to create multiple RMEPs in multiple MDs, repeat [Step 2](#) to [Step 4](#).

1.6.7 (Optional) Setting the Rule for Creating a MIP

Context

Do as follows on the S-switch that requires Ethernet CFM:

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **mip create-type { default | explicit | none } [interface interface-type interface-number]** command to set the rule for creating a MIP.

By default, the rule for creating a MIP globally is **none**. The rule for creating a MIP globally is the same as the rule for creating a MIP on the interface. Comply with the rule for creating a MIP if the rule is configured on interfaces.

- **default**: MIPs can be created on an interface without a MEP of a higher level or a MIP of a lower level.
- **explicit**: MIPs cannot be created on an interface without a MEP of a lower level. MIPs can be created on an interface without a MEP of a higher level or a MIP of a lower level.
- **none**: MIPs cannot be created on an interface.

If the rule for creating the MIP is default or explicit, the device creates the MIP automatically according to the rule.

----End

1.6.8 Enabling CC Detection

Context

Do as follows on the edge devices on which MEPs reside within MAs:

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **cfm md md-name** command to enter the MD view.

Step 3 Run the **ma ma-name** command to enter the MA view.

Step 4 Run the **ccm-interval interval** command to set the interval for the MEP sending or detecting CCMs within the local MA.

By default, the interval for the MEP sending or detecting CCMs within an MA is 1 second.

- The sending of CCMs is enabled by using the **mep ccm-send enable** command.
- The receiving of CCMs is enabled by using the **remote-mep ccm-receive enable** command.

If any of the preceding conditions is met in an MA, the interval for sending or detecting CCMs in the MA cannot be modified. If you want to modify the interval for sending or detecting CCMs in an MA, you must run the related **undo** commands to disable the sending or receiving of CCMs.

Step 5 Run the **mep ccm-send [mep-id mep-id] enable** command to enable the sending of CCMs on the MEP.

By default, a MEP is disabled to send CCMs.

If **mep-id mep-id** is not specified, all the MEPs in the MA are enabled to send CCMs.

Step 6 Run the **remote-mep ccm-receive [mep-id mep-id] enable** command to enable the receiving of CCMs from the RMEP within the same MA on the local MEP.

By default, the local MEP cannot receive CCMs from the RMEP.

When the local device is enabled to receive CCMs from an RMEP, and if connectivity faults are detected between the local device and the RMEP through CC detection, the local device prompts alarms of RMEP connectivity.

If **mep-id mep-id** is not specified, all the MEPs in the MA are enabled to receive CCMs from all the RMEPs.

----End

Postrequisite

- If you need to enable the CC detection in multiple MAs, repeat [Step 3](#) to [Step 6](#).
- If you need to enable the CC detection in multiple MDs, repeat [Step 2](#) to [Step 6](#).

1.6.9 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the configuration information about an MD.	display cfm md [<i>md-name</i>]
Check detailed information about an MA.	display cfm ma [md <i>md-name</i> [ma <i>ma-name</i>]]
Check detailed information about a MEP.	display cfm mep [md <i>md-name</i> [ma <i>ma-name</i> [mep-id <i>mep-id</i>]]]
Check detailed information about an RMEP.	display cfm remote-mep [md <i>md-name</i> [ma <i>ma-name</i> [mep-id <i>mep-id</i>]]]
Check the rule for creating a MIP.	display mip create-type [interface <i>interface-type</i> <i>interface-number</i>]
Check information about a MIP.	display cfm mip [interface <i>interface-type</i> <i>interface-number</i> level <i>level</i>]

Run the **display cfm md** command. If the MD and the level of the MD are displayed, it means that the configuration succeeds.

```
<Quidway> display cfm md
MD-Name  Level
-----
md2      7
md3      3
```

Run the **display cfm ma** command. If information about the MA is displayed, it means that the configuration succeeds.

```
<Quidway> display cfm ma
MD Name      : md2
Level        : 7
MA Name      : ma3
Interval     : 10ms
Priority     : 4
Vlan ID     : 17
MEP Number   : 2
RMEP Number  : 1
MD Name      : md3
Level        : 3
MA Name      : ma3
Interval     : 1000ms
Priority     : 5
Vlan ID     : 18
MEP Number   : 1
RMEP Number  : 1
```

Run the **display cfm mep** command. If information about the MEP is displayed, it means that the configuration succeeds.

```
<Quidway> display cfm mep
MD Name      : md2
Level        : 7
MA Name      : ma3
```

```
MEP ID          : 40
Vlan ID         : 10
Interface Name  : GigabitEthernet0/0/1
CCM Send       : enabled
Direction      : outward

MD Name         : md3
Level          : 3
MA Name        : ma1
MEP ID         : 100
Vlan ID        : 20
Interface Name  : GigabitEthernet0/0/1
CCM Send       : enabled
Direction      : outward
```

Run the **display cfm remote-mep** command. If information about the RMEP is displayed, it means that the configuration succeeds.

```
<Quidway> display cfm remote-mep
The total number of RMEPs is 2
MD Name          : md2
Level           : 7
MA Name         : ma3
RMEP ID         : 110
Vlan ID         : 20
MAC             : 0000-0121-0222
CCM Receive     : enabled
CFM Status      : up
RDI             : 0
MACSTATUS:      : 0
REMOTECC:       : 0
ERRORCC:        : 0
XCONCC:         : 0
start-delay     : 180 seconds

MD Name          : md2
Level           : 4
MA Name         : ma3
RMEP ID         : 30
Vlan ID         : --
MAC             : --
CCM Receive     : enabled
CFM Status      : up
RDI             : 0
MACSTATUS:      : 0
REMOTECC:       : 0
ERRORCC:        : 0
XCONCC:         : 0
start-delay     : 180 seconds
```

Run the **display mip create-type** command. If the rule for creating the MIP is correct, it means that the configuration succeeds.

```
<Quidway> display mip create-type interface gigabitethernet1/0/1
Interface Name      MIP Create-Type  MIP Create-Type On Interface
-----
GigabitEthernet0/0/1  none                               --
```

Run the **display cfm mip** command. If information about the MIP is displayed, it means that the configuration succeeds.

```
<Quidway> display cfm mip
Interface Name      Level
-----
ethernet0/0/1      7
ethernet0/0/2      6
```

1.7 Fault Verification on the Ethernet

This section describes the method of testing the connectivity on the Ethernet through 802.1ag MAC ping or MAC ping.

[1.7.1 Establishing the Configuration Task](#)

[1.7.2 \(Optional\) Implementing 802.1ag MAC Ping](#)

[1.7.3 \(Optional\) Implementing MAC Ping](#)

1.7.1 Establishing the Configuration Task

Applicable Environment

To manually detect the connectivity between two devices, you can send test packets and wait for a reply to test whether the destination device is reachable. There are the following scenarios based on the type of the link to be tested:

- For the network where the MD, MA, and MEP are configured, you can implement 802.1ag MAC ping to test the connectivity between MEPs at the same maintenance level or between MEPs and MIPs at the same maintenance level.
- For the network where the MD, MA, and MEP are not configured, you can implement MAC ping to test the connectivity between two devices.

Pre-configuration Tasks

Before implementing 802.1ag MAC ping, complete the following tasks:

- [Configuring Ethernet CFM](#)

No pre-configuration tasks are needed to implement MAC ping.

Data Preparation

To detect the connectivity on the Ethernet, you need the following data.

No.	Data
1	(Optional) Bridge MAC address of the device on which the destination MEP resides or ID of the destination MEP
2	(Optional) Bridge MAC address of the device on which the destination MIP resides
3	(Optional) Number, size, timeout period, and outbound interface of LBMs
4	(Optional) VLAN to which the destination node belongs

1.7.2 (Optional) Implementing 802.1ag MAC Ping

Context

Do as follows on the S-switch with a MEP at one end of the link to be tested:

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **cfm md md-name** command to enter the MD view.
- Step 3** Run the **ma ma-name** command to enter the MA view.
- Step 4** Run the **ping mac-8021ag { mac mac-address | remote-mep mep-id mep-id } [-c count | -s packet-size | -t timeout | interface interface-type interface-number] *** command to test the connectivity between a MEP and a MEP or a MIP on other devices.

When implementing 802.1ag MAC ping, ensure that:

- The MA is associated with a VLAN.
- The MEP is configured in the MA.
- If the outbound interface is specified, it cannot be configured with an inward-facing MEP. The interface must be added to the VLAN associated with the MA.
- If the destination node is a MEP, either **mac mac-address** or **remote-mep mep-id mep-id** can be selected. If **remote-mep mep-id mep-id** is selected, the RMEP must already be created with the **remote-mep** command and the bridge MAC address of the device on which the RMEP resides must be specified.
- If the destination node is a MIP, select **mac mac-address**.

The intermediate device on the link to be tested only forwards LBMs and LBRs. In this manner, the MD, MA, or MEP are not required to be configured on the intermediate device.

----End

1.7.3 (Optional) Implementing MAC Ping

Context

Perform Step 1 and Step 2 on the S-switches at both ends of the link to be tested. Perform Step 3 on any of the S-switches.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ping mac enable** command to enable MAC ping globally.

By default, MAC ping is disabled.

When MAC ping is enabled:

- MAC ping can be implemented on the S-switches.

- The S-switches can respond to LBMs.

Step 3 Run the **ping mac** *mac-address* **vlan** *vlan-id* [**-c** *count* | **-s** *packet-size* | **-t** *timeout* | **interface** *interface-type interface-number*] * command to test the connectivity between the S-switch and the remote device.

A MEP is not required to initiate MAC ping. The destination node does not need to be a MEP or a MIP. MAC ping can be implemented without configuring the MD, MA, or MEP on the source device, the intermediate device, and the destination device.

----End

1.8 Locating the Fault on the Ethernet

This section describes the method of locating the connectivity fault on the Ethernet through 802.1ag MAC trace or MAC trace.

1.8.1 Establishing the Configuration Task

1.8.2 (Optional) Implementing 802.1ag MAC Trace

1.8.3 (Optional) Implementing MAC Trace

1.8.1 Establishing the Configuration Task

Applicable Environment

To locate the connectivity fault between two devices, you can send test packets and wait for reply packets to test the path between the local device and the destination device and to locate faults. There are the following scenarios based on what kind of link is being tested:

- For the network where the MD, MA, and MEP are configured, you can implement 802.1ag MAC trace to locate the connectivity fault between MEPs at the same maintenance level or between MEPs and MIPs at the same maintenance level.
- For the network where the MD, MA, and MEP are not configured, you can implement MAC trace to locate the connectivity fault between two devices.

Pre-configuration Tasks

Before implementing 802.1ag MAC trace, complete the following tasks:

- **Configuring Ethernet CFM**

No pre-configuration tasks are needed to implement MAC trace.

Data Preparation

To locate the connectivity fault on the Ethernet, you need the following data.

No.	Data
1	(Optional) Bridge MAC address of the device on which the destination MEP resides or ID of the destination MEP

No.	Data
2	(Optional) Bridge MAC address of the device on which the destination MIP resides
3	(Optional) Outbound interface of Linktrace Messages (LTMs)
4	(Optional) Timeout period for waiting for an LTR
5	(Optional) Time to Live (TTL) of LTMs
6	(Optional) VLAN to which the destination node belongs

1.8.2 (Optional) Implementing 802.1ag MAC Trace

Context

Do as follows on the S-switch with a MEP at one end of the link to be tested:

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **cfm md md-name** command to enter the MD view.
- Step 3** Run the **ma ma-name** command to enter the MA view.
- Step 4** Run the **trace mac-8021ag { mac mac-address | remote-mep mep-id mep-id } [interface interface-type interface-number | -t timeout | ttl ttl] *** command to locate the connectivity fault between the S-switch and the remote S-switch.

When implementing 802.1ag MAC trace, ensure that:

- The MA is associated with a VLAN.
- The MEP is configured in the MA.
- If the outbound interface is specified, it cannot be configured with an inward-facing MEP. The interface must be added to the VLAN associated with the MA.
- If the destination node is a MEP, either **mac mac-address** or **remote-mep mep-id mep-id** can be selected. If **remote-mep mep-id mep-id** is selected, the RMEP must already be created with the **remote-mep** command and the bridge MAC address of the device on which the RMEP resides must be specified.
- If the destination node is a MIP, select **mac mac-address**.
- If the forwarding entry of the destination node does not exist in the MAC address table, **interface interface-type interface-number** must be specified.

The intermediate device on the link to be tested only forwards LTMs and LTRs. In this manner, the MD, MA, or MEP are not required to be configured on the intermediate device.

----End

1.8.3 (Optional) Implementing MAC Trace

Context

You need to configure the S-switches at both ends and the intermediate S-switch on the link to be tested.

Procedure

Step 1 Configuring the S-switches at both Ends and the Intermediate S-switch

Do as follows on the S-switches at both ends and the intermediate S-switch on the link to be tested:

1. Run the **system-view** command to enter the system view.
2. Run the **trace mac enable** command to enable MAC trace globally.

By default, MAC trace is disabled.

The following can be performed only after MAC trace is enabled:

- MAC trace can be implemented on the S-switch.
- The S-switches can respond to LTMs of MAC trace.

Step 2 Implementing MAC Trace

Do as follows on the S-switch at one end of the link to be tested:

1. Run the **system-view** command to enter the system view.
2. Run the **trace mac mac-address vlan vlan-id [interface interface-type interface-number [-t timeout] *** command to locate the connectivity fault between the S-switch and the remote S-switch.

A MEP is not required to initiate MAC trace. The destination node does not need to be a MEP or a MIP. MAC trace can be implemented without configuring the MD, MA, or MEP on the source device, the intermediate device, and the destination device.

----End

1.9 Maintaining Ethernet OAM

This section describes how to debug EFM OAM, how to monitor the running status of Ethernet OAM, and how to clear the statistics on error CCMs.

[1.9.1 Clearing the Statistics on Error CCMs](#)

[1.9.2 Debugging EFM OAM](#)

[1.9.3 Monitoring the Running Status of Ethernet OAM](#)

1.9.1 Clearing the Statistics on Error CCMs

To clear the history statistics when you need to observe statistics of error CCMs in a period from the current time, run the following **reset** command in the user view.

Action	Command
Clear statistics of error CCMs.	reset cfm error-packet receive statistics [md <i>md-name</i> [ma <i>ma-name</i> [remote-mep <i>mep-id</i> <i>mep-id</i>]]]

1.9.2 Debugging EFM OAM



CAUTION

Debugging affects the performance of the system. So, after debugging, run the **undo debugging all** command to disable it immediately.

When an EFM OAM fault occurs, run the following **debugging** command in the user view to view the debugging information, and locate and analyze the fault.

For the procedure of displaying the debugging information, refer to the chapter "Debugging and Diagnosis" in the *Quidway S5300 Series Ethernet Switches Configuration Guide - Device Management*.

Action	Command
Enable the debugging of the EFM OAM module on a specified interface.	debugging efm interface <i>interface-type</i> <i>interface-number</i> { all error message packet { all receive send } process }

1.9.3 Monitoring the Running Status of Ethernet OAM

To check the running status of Ethernet OAM during routine maintenance, run the following **display** command in any view.

Action	Command
Check information about the EFM OAM session between a specified interface and the peer.	display efm session { all interface <i>interface-type</i> <i>interface-number</i> }

1.10 Configuration Examples

This section provides several configuration examples of Ethernet OAM.

[1.10.1 Example for Configuring EFM OAM](#)

[1.10.2 Example for Testing the Packet Loss Ratio on a Link](#)

1.10.3 Example for Configuring Ethernet CFM

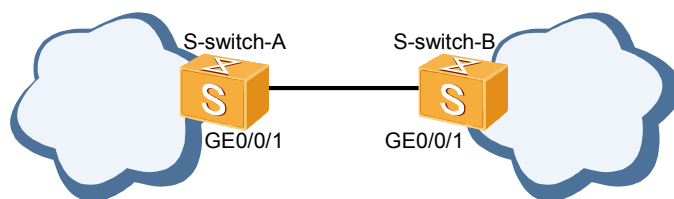
1.10.1 Example for Configuring EFM OAM

Networking Requirements

As shown in **Figure 1-4**, S-switch-A and S-switch-B are connected through GE 0/0/1. It is required that the following be achieved:

- Automatic connectivity detection can be performed between S-switch-A and S-switch-B. After detecting connectivity faults, S-switch-A and S-switch-B generate alarms.
- When any of the following faults occurs on S-switch-A or S-switch-B, the other device can receive the fault notification messages and generate an alarm:
 - The system reboots.
 - A physical link fails.
 - OAMPDUs time out.
- S-switch-B monitors the errored frames, errored codes, and errored frame seconds on GE 0/0/1. When the number of errored frames, errored codes, or errored frame seconds exceeds the set threshold, S-switch-B generates an alarm.

Figure 1-4 Networking for configuring EFM OAM



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable EFM OAM globally on S-switch-A and S-switch-B.
2. Configure EFM OAM on GE 0/0/1 of S-switch-A to work in passive mode.
3. Configure GE 0/0/1 on S-switch-B to detect the errored frames, errored codes, and errored frame seconds.
4. Enable EFM OAM on GE 0/0/1 of S-switch-A and S-switch-B respectively.

Data Preparation

To complete the configuration, you need the following data:

- The period for detecting errored frames on GE 0/0/1 of S-switch-B is 5 seconds, and the threshold is 5.
- The period for detecting errored codes on GE 0/0/1 of S-switch-B is 5 seconds, and the threshold is 5.
- The period for detecting errored frame seconds on GE 0/0/1 of S-switch-B is 120 seconds, and the threshold is 5.

Configuration Procedure

1. Enable EFM OAM globally.
Enable EFM OAM globally on S-switch-A.

```
<Quidway> system-view
[Quidway] sysname S-switch-A
[S-switch-A] efm enable
```


Enable EFM OAM globally on S-switch-B.

```
<Quidway> system-view
[Quidway] sysname S-switch-B
[S-switch-B] efm enable
```
2. Configure EFM OAM on GE 0/0/1 of S-switch-A to work in passive mode.

```
[S-switch-A] interface gigabitethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] efm mode passive
```
3. Configure GE 0/0/1 on S-switch-B to detect errored frames, errored codes, and errored frame seconds.
Configure GE 0/0/1 on S-switch-B to detect errored frames.

```
[S-switch-B] interface gigabitethernet 0/0/1
[S-switch-B-GigabitEthernet0/0/1] efm error-frame period 5
[S-switch-B-GigabitEthernet0/0/1] efm error-frame threshold 5
[S-switch-B-GigabitEthernet0/0/1] efm error-frame notification enable
```


Configure GE 0/0/1 on S-switch-B to detect errored codes.

```
[S-switch-B-GigabitEthernet0/0/1] efm error-code period 5
[S-switch-B-GigabitEthernet0/0/1] efm error-code threshold 5
[S-switch-B-GigabitEthernet0/0/1] efm error-code notification enable
```


Configure GE 0/0/1 on S-switch-B to detect errored frame seconds.

```
[S-switch-B-GigabitEthernet0/0/1] efm error-frame-second period 120
[S-switch-B-GigabitEthernet0/0/1] efm error-frame-second threshold 5
[S-switch-B-GigabitEthernet0/0/1] efm error-frame-second notification enable
```
4. Enable EFM OAM on GE 0/0/1 of S-switch-A and S-switch-B respectively.
Enable EFM OAM on GE 0/0/1 of S-switch-A.

```
[S-switch-A-GigabitEthernet0/0/1] efm enable
[S-switch-A-GigabitEthernet0/0/1] bpdu enable
[S-switch-A-GigabitEthernet0/0/1] quit
```


Enable EFM OAM on GE 0/0/1 of S-switch-B.

```
[S-switch-B-GigabitEthernet0/0/1] efm enable
[S-switch-B-GigabitEthernet0/0/1] quit
```
5. Verify the configuration.
Run the **display efm session** command. If the EFM OAM status on the interfaces is Detect, it means that the configuration succeeds. EFM OAM is correctly configured on S-switch-A and S-switch-B, and interfaces GE 0/0/1 succeed in negotiation and enter the Detect state. For example, the EFM OAM status on GE 0/0/1 of S-switch-B is displayed as follows:

```
<S-switch-B> display efm session interface gigabitethernet 0/0/1
  Interface                EFM State      Loopback Timeout
  -----
  GigabitEthernet0/0/1      detect         --
```


Run the **display efm** command. If the EFM OAM configuration on GE 0/0/1 of S-switch-B is displayed, it means that the configuration succeeds. The displayed information is as follows:

```
<S-switch-B> display efm interface gigabitethernet 0/0/1
  Item                      Value
  -----
  Interface:                GigabitEthernet0/0/1
```

```
EFM Enable Flag:          enable
Mode:                     active
OAMPDU MaxSize:           128
ErrCodeNotification:      enable
ErrCodePeriod:            5
ErrCodeThreshold:         5
ErrFrameNotification:      enable
ErrFramePeriod:           5
ErrFrameThreshold:        5
ErrFrameSecondNotification: enable
ErrFrameSecondPeriod:     120
ErrFrameSecondThreshold:  5
TriggerIfDown:            disable
Remote MAC:               0010-0010-0010
Remote EFM Enable Flag:   enable
Remote Mode:              passive
Remote MaxSize:           128
```

Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
efm enable
#
interface GigabitEthernet0/0/1
efm mode passive
efm enable
bpdu enable
#
return
```

- Configuration file of S-switch-B

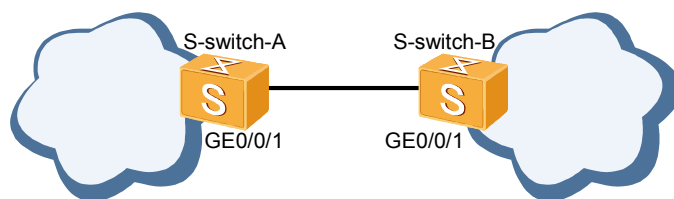
```
#
sysname S-switch-B
#
efm enable
#
interface GigabitEthernet0/0/1
efm enable
efm error-frame period 5
efm error-frame threshold 5
efm error-frame notification enable
efm error-frame-second period 120
efm error-frame-second threshold 5
efm error-frame-second notification enable
efm error-code period 5
efm error-code threshold 5
efm error-code notification enable
#
return
```

1.10.2 Example for Testing the Packet Loss Ratio on a Link

Networking Requirements

As shown in [Figure 1-5](#), the link between S-switch-A and S-switch-B is newly established. The ISP needs to test the packet loss ratio on the link on S-switch-B before using the link.

Figure 1-5 Networking for testing the packet loss ratio on a link



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable EFM OAM on S-switch-A and S-switch-B. Configure EFM OAM on GE 0/0/1 of S-switch-A to work in passive mode.
2. Configure EFM OAM remote loopback on S-switch-B.
3. Send test packets from S-switch-B to S-switch-A.
4. Collect the statistics on received test packets on S-switch-B.

Data Preparation

To complete the configuration, you need the following data:

- Timeout period for EFM OAM remote loopback
- Size, number, and transmission rate of test packets

Configuration Procedure

1. Configure EFM OAM.

Enable EFM OAM globally on S-switch-A.

```
<Quidway> system-view
[Quidway] sysname S-switch-A
[S-switch-A] efm enable
```

Enable EFM OAM globally on S-switch-B.

```
<Quidway> system-view
[Quidway] sysname S-switch-B
[S-switch-B] efm enable
```

Configure EFM OAM on GE 0/0/1 of S-switch-A to work in passive mode.

```
[S-switch-A] interface gigabitethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] efm mode passive
```

Enable EFM OAM on GE 0/0/1 of S-switch-A.

```
[S-switch-A-GigabitEthernet0/0/1] efm enable
[S-switch-A-GigabitEthernet0/0/1] bpdu enable
[S-switch-A-GigabitEthernet0/0/1] quit
```

Enable EFM OAM on GE 0/0/1 of S-switch-B.

```
[S-switch-B] interface gigabitethernet 0/0/1
[S-switch-B-GigabitEthernet0/0/1] efm enable
[S-switch-B-GigabitEthernet0/0/1] quit
```

Verify the configuration.

Run the **display efm session** command. If the EFM OAM protocol on GE 0/0/1 is in the Detect state, it means that the configuration succeeds. EFM OAM is correctly configured on S-switch-A and S-switch-B, and interfaces GE 0/0/1 succeed in negotiation and enter

the Detect state. For example, the EFM OAM status on GE 0/0/1 of S-switch-B is displayed as follows:

```
[S-switch-B] display efm session interface gigabitethernet 0/0/1
Interface                      EFM State                      Loopback Timeout
-----
GigabitEthernet0/0/1          detect                          --
```

2. Configure EFM OAM remote loopback.

Configure EFM OAM remote loopback on S-switch-B.

```
[S-switch-B] interface gigabitethernet 0/0/1
[S-switch-B-GigabitEthernet0/0/1] efm loopback start
[S-switch-B-GigabitEthernet0/0/1] quit
```

Verify the configuration.

Run the **display efm session** command on S-switch-B. If the EFM OAM protocol on GE 0/0/1 is in the Loopback (control) state, that is, GE 0/0/1 initiates remote loopback, it means that the configuration succeeds. The displayed information is as follows:

```
[S-switch-B] display efm session interface gigabitethernet0/0/1
Interface                      EFM State                      Loopback Timeout
-----
GigabitEthernet0/0/1          loopback(control)              20
```

Run the **display efm session** command on S-switch-A. If the EFM OAM protocol on GE 0/0/1 is in the Loopback (be controlled) state, that is, GE 0/0/1 responds to remote loopback, it means that the configuration succeeds. The displayed information is as follows:

```
[S-switch-A] display efm session interface gigabitethernet0/0/1
Interface                      EFM State                      Loopback Timeout
-----
GigabitEthernet0/0/1          loopback(be controlled)        --
```

3. Send test packets from S-switch-B to S-switch-A.

```
[S-switch-B] test-packet start interface gigabitethernet 0/0/1
Info: This operation will take some time. Please wait.....succeeded.
```

4. Collect the statistics on received test packets on S-switch-B.

```
[S-switch-B] display test-packet result
Test Item                      Test Result
-----
PacketsSend                    :          5
PacketsReceive                 :          5
PacketsLost                    :           0
BytesSend                      :         320
BytesReceive                   :         320
BytesLost                      :           0
StartTime                     : 07:06:2008 09:41:41
EndTime                       : 07:06:2008 09:41:42
```

You can obtain the packet loss ratio on the link based on the preceding data.

5. Disable EFM OAM remote loopback.

Disable EFM OAM remote loopback on S-switch-B.

```
[S-switch-B] interface gigabitethernet 0/0/1
[S-switch-B-GigabitEthernet0/0/1] efm loopback stop
[S-switch-B-GigabitEthernet0/0/1] quit
```

By default, the timeout period for remote loopback is 20 minutes. After 20 minutes, remote loopback stops. To disable remote loopback, you can perform the preceding steps.

Verify the configuration.

Run the **display efm session** command after remote loopback is automatically or manually disabled, you can view that the status of the EFM OAM protocol on the interface is no longer Loopback (control) or Loopback (be controlled). For example, the EFM OAM status on GE 0/0/1 of S-switch-B is displayed as follows:

```
[S-switch-B] display efm session interface gigabitethernet0/0/1
Interface                EFM State                Loopback Timeout
-----
GigabitEthernet0/0/1    detect                    --
```

Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
 efm enable
#
interface GigabitEthernet0/0/1
 efm mode passive
 efm enable
 bpdu enable
#
return
```

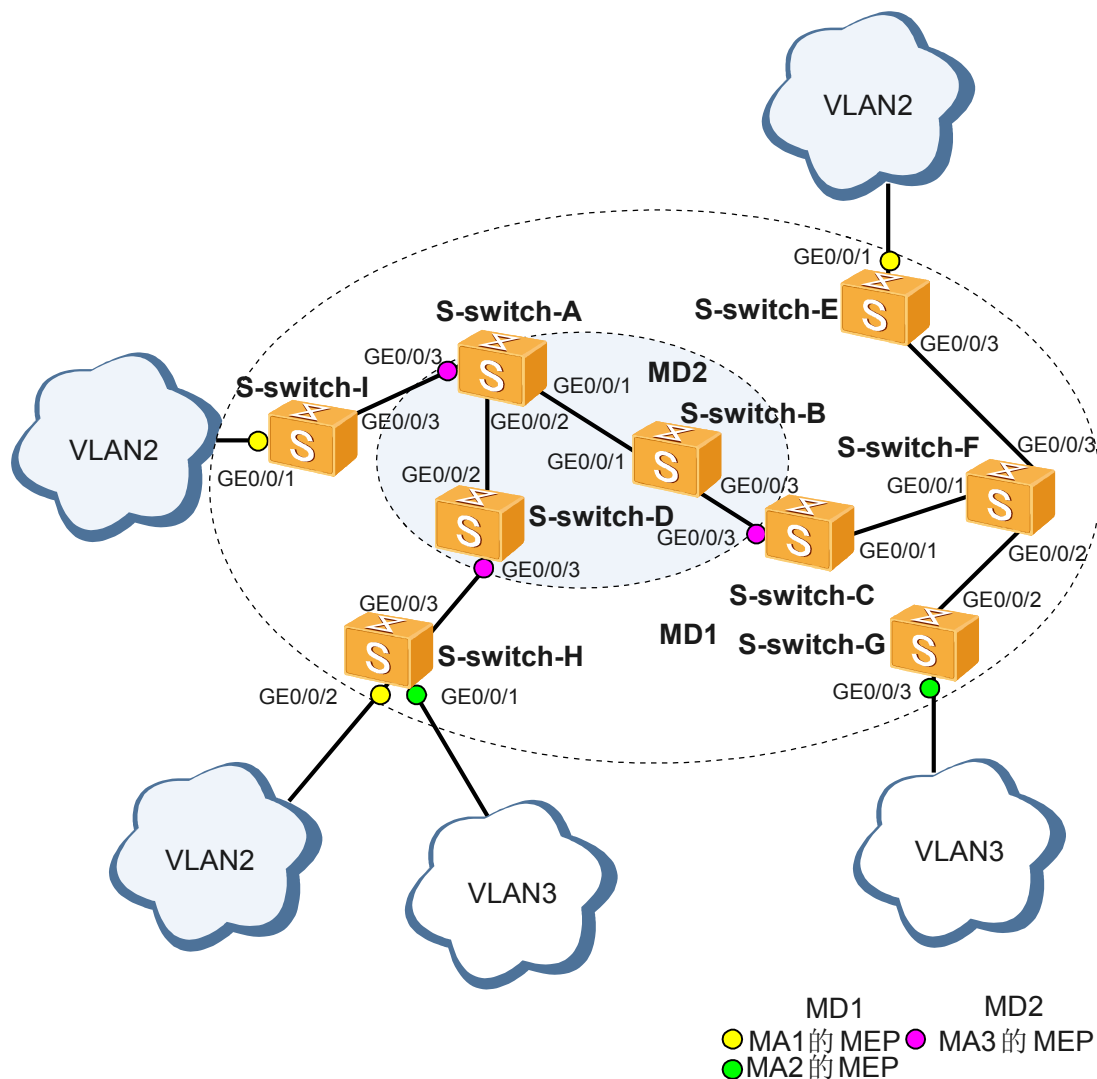
- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
 efm enable
#
interface GigabitEthernet0/0/1
 efm enable
#
return
```

1.10.3 Example for Configuring Ethernet CFM

Networking Requirements

The Ethernet shown in [Figure 1-6](#) is managed by two ISPs. ISP 1 manages S-switch-A, S-switch-B, and S-switch-D. ISP 2 manages S-switch-C, S-switch-E, S-switch-F, S-switch-G, S-switch-H, and S-switch-I. It is required that connectivity detection be implemented on the network.

Figure 1-6 Diagram of configuring Ethernet CFM

Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and add interfaces to the corresponding VLAN.
2. Create MD 1 at level 6 on all the S-switch-s.
3. Create MA 1 within MD 1 on all the S-switch-s except S-switch-G. Associate MA 1 with VLAN 2.
4. Create MA 2 within MD 1 on all the S-switch-s except S-switch-E and S-switch-I. Associate MA 2 with VLAN 3.
5. Create MD 2 at level 4 on S-switch-A, S-switch-B, S-switch-C, and S-switch-D. Create MA 3 within MD 2. Associate MA 3 with VLAN 4.
6. Create MEPs and RMEPs on S-switch-I, S-switch-H, and S-switch-E in MA 1 within MD 1.
7. Create MEPs and RMEPs on S-switch-H and S-switch-G in MA 2 within MD 1.

8. Create MEPs and RMEPs on S-switch-A, S-switch-C, and S-switch-D in MA 3 within MD 2.
9. Enable the sending and receiving of CCMs.

Data Preparation

To complete the configuration, you need the following data:

- MD 1 at level 6
- MD 2 at level 4

Configuration Procedure

1. Create VLANs and add interfaces to the corresponding VLAN. The detailed configuration is not mentioned here.
2. Create MD 1.

Create MD 1 on S-switch-A.

```
<S-switch-A> system-view
[S-switch-A] cfm enable
Info: Succeeded in enabling CFM.
[S-switch-A] cfm md md1 level 6
```

Create MD 1 on S-switch-B, S-switch-C, S-switch-D, S-switch-E, S-switch-F, S-switch-G, S-switch-H, and S-switch-I.

The detailed configuration is not mentioned here. The configuration is similar to that on S-switch-A.

3. Create and configure MA 1 within MD 1 on all the device except S-switch-G.

Create and configure MA 1 on S-switch-A within MD 1.

```
[S-switch-A-md-md1] ma ma1
[S-switch-A-md-md1-ma-ma1] map vlan 2
[S-switch-A-md-md1-ma-ma1] quit
```

Create and configure MA 1 on S-switch-B, S-switch-C, S-switch-D, S-switch-E, S-switch-F, S-switch-H, and S-switch-I within MD 1.

The detailed configuration is not mentioned here. The configuration is similar to that on S-switch-A.

4. Create and configure MA 2 within MD 1 on all the device except S-switch-E and S-switch-I.

Create and configure MA 2 on S-switch-A within MD 1.

```
[S-switch-A-md-md1] ma ma2
[S-switch-A-md-md1-ma-ma2] map vlan 3
[S-switch-A-md-md1-ma-ma2] quit
[S-switch-A-md-md1] quit
```

Create and configure MA 2 on S-switch-B, S-switch-C, S-switch-D, S-switch-F, S-switch-G, and S-switch-H within MD 1.

The detailed configuration is not mentioned here. The configuration is similar to that on S-switch-A.

5. Create MD 2 on S-switch-A, S-switch-B, S-switch-C, and S-switch-D. Create and configure MA 3 within MD 2.

Create MD 2 on S-switch-A. Create and configure MA 3 within MD 2.

```
[S-switch-A] cfm md md2 level 4
[S-switch-A-md-md2] ma ma3
```

```
[S-switch-A-md-md2-ma-ma3] map vlan 4
[S-switch-A-md-md2-ma-ma3] quit
[S-switch-A-md-md2] quit
```

Create MD 2 on S-switch-B, S-switch-C, and S-switch-D. Create and configure MA 3 within MD 2.

The detailed configuration is not mentioned here. The configuration is similar to that on S-switch-A.

6. Configure MEPs and RMEPs on S-switch-E, S-switch-H, and S-switch-I in MA 1 within MD 1.

Configure a MEP on S-switch-E in MA 1 within MD 1.

```
[S-switch-E] cfm md md1
[S-switch-E-md-md1] ma ma1
[S-switch-E-md-md1-ma-ma1] mep mep-id 3 interface tethernet 0/0/1 inward
```

Configure a MEP on S-switch-H in MA 1 within MD 1.

```
[S-switch-H] cfm md md1
[S-switch-H-md-md1] ma ma1
[S-switch-H-md-md1-ma-ma1] mep mep-id 2 interface ethernet 0/0/2 inward
```

Configure a MEP on S-switch-I in MA 1 within MD 1.

```
[S-switch-I] cfm md md1
[S-switch-I-md-md1] ma ma1
[S-switch-I-md-md1-ma-ma1] mep mep-id 1 interface ethernet 0/0/1 inward
```

Configure an RMEP on S-switch-E in MA 1 within MD 1.

```
[S-switch-E-md-md1-ma-ma1] remote-mep mep-id 1
[S-switch-E-md-md1-ma-ma1] remote-mep mep-id 2
```

Configure an RMEP on S-switch-H in MA 1 within MD 1.

```
[S-switch-H-md-md1-ma-ma1] remote-mep mep-id 1
[S-switch-H-md-md1-ma-ma1] remote-mep mep-id 3
```

Configure an RMEP on S-switch-I in MA 1 within MD 1.

```
[S-switch-I-md-md1-ma-ma1] remote-mep mep-id 2
[S-switch-I-md-md1-ma-ma1] remote-mep mep-id 3
```

7. Configure MEPs and RMEPs on S-switch-H and S-switch-G in MA 2 within MD 1.

Configure a MEP on S-switch-H in MA 2 within MD 1.

```
[S-switch-H] cfm md md1
[S-switch-H-md-md1] ma ma2
[S-switch-H-md-md1-ma-ma2] mep mep-id 1 interface ethernet 0/0/1 inward
```

Configure a MEP on S-switch-G in MA 2 within MD 1.

```
[S-switch-G] cfm md md1
[S-switch-G-md-md1] ma ma2
[S-switch-G-md-md1-ma-ma2] mep mep-id 2 interface GigabitEthernet 0/0/3 inward
```

Configure an RMEP on S-switch-H in MA 2 within MD 1.

```
[S-switch-H-md-md1-ma-ma2] remote-mep mep-id 2
```

Configure an RMEP on S-switch-G in MA 2 within MD 1.

```
[S-switch-G-md-md1-ma-ma2] remote-mep mep-id 1
```

8. Configure MEPs and RMEPs on S-switch-A, S-switch-C, and S-switch-D in MA 3 within MD 2.

Configure a MEP on S-switch-A in MA 3 within MD 2.

```
[S-switch-A] cfm md md2
[S-switch-A-md-md2] ma ma3
[S-switch-A-md-md2-ma-ma3] mep mep-id 1 interface GigabitEthernet 0/0/3 inward
```

Configure a MEP on S-switch-C in MA 3 within MD 2.

```
[S-switch-C] cfm md md2
```

- ```
[S-switch-C-md-md2] ma ma3
[S-switch-C-md-md2-ma-ma3] mep mep-id 2 interface GigabitEthernet 0/0/1 outward
```
- # Configure a MEP on S-switch-D in MA 3 within MD 2.
- ```
[S-switch-D] cfm md md2
[S-switch-D-md-md2] ma ma3
[S-switch-D-md-md2-ma-ma3] mep mep-id 3 interface GigabitEthernet 0/0/3 inward
```
- # Configure an RMEP on S-switch-A in MA 3 within MD 2.
- ```
[S-switch-A-md-md2-ma-ma3] remote-mep mep-id 2
[S-switch-A-md-md2-ma-ma3] remote-mep mep-id 3
```
- # Configure an RMEP on S-switch-C in MA 3 within MD 2.
- ```
[S-switch-C-md-md2-ma-ma3] remote-mep mep-id 1
[S-switch-C-md-md2-ma-ma3] remote-mep mep-id 3
```
- # Configure an RMEP on S-switch-D in MA 3 within MD 2.
- ```
[S-switch-D-md-md2-ma-ma3] remote-mep mep-id 1
[S-switch-D-md-md2-ma-ma3] remote-mep mep-id 2
```
9. Enable the sending and receiving of CCMs.
- # Enable the sending of CCMs on the MEP on S-switch-A.
- ```
[S-switch-A-md-md2-ma-ma3] mep ccm-send enable
```
- # Enable the receiving of CCMs from the RMEP on S-switch-A.
- ```
[S-switch-A-md-md2-ma-ma3] remote-mep ccm-receive enable
```
- # Enable the sending of CCMs on MEPs and the receiving of CCMs from RMEPs on S-switch-B, S-switch-C, S-switch-D, S-switch-E, S-switch-F, S-switch-G, S-switch-H, and S-switch-I.
- The detailed configuration is not mentioned here. The configuration is similar to that on S-switch-A.

## Configuration Files

- Configuration file of S-switch-A
 

```
#
sysname S-switch-A
#
vlan batch 2 to 4
#
cfm enable
#
interface GigabitEthernet0/0/3
 port trunk allow-pass vlan 2 to 4
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 2 to 4
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 2 to 4
#
cfm md md1 level 6
 ma ma1
 map vlan 2
 ma ma2
 map vlan 3
#
cfm md md2 level 4
 ma ma3
 map vlan 4
 mep mep-id 1 interface GigabitEthernet 0/0/3 inward
 mep ccm-send mep-id 1 enable
 remote-mep mep-id 2
 remote-mep ccm-receive mep-id 2 enable
 remote-mep mep-id 3
```

```
 remote-mep ccm-receive mep-id 3 enable
#
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
vlan batch 2 to 4
#
cfm enable
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 2 to 4
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 2 to 4
#
cfm md md1 level 6
ma ma1
map vlan 2
ma ma2
map vlan 3
#
cfm md md2 level 4
ma ma3
map vlan 4
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
vlan batch 2 to 4
#
cfm enable
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 2 to 4
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 2 to 4
#
cfm md md1 level 6
ma ma1
map vlan 2
ma ma2
map vlan 3
#
cfm md md2 level 4
ma ma3
map vlan 4
mep mep-id 2 interface GigabitEthernet 0/0/3 outward
mep ccm-send mep-id 2 enable
remote-mep mep-id 1
remote-mep ccm-receive mep-id 1 enable
remote-mep mep-id 3
remote-mep ccm-receive mep-id 3 enable
#
return
```

- Configuration file of S-switch-D

```
#
sysname S-switch-D
#
vlan batch 2 to 4
#
cfm enable
#
```

```
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 2 to 4
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 2 to 4
#
cfm md md1 level 6
ma ma1
map vlan 2
ma ma2
map vlan 3
#
cfm md md2 level 4
ma ma3
map vlan 4
mep mep-id 3 interface GigabitEthernet 0/0/3 inward
mep ccm-send mep-id 3 enable
remote-mep mep-id 1
remote-mep ccm-receive mep-id 1 enable
remote-mep mep-id 1
remote-mep ccm-receive mep-id 2 enable
#
return
```

- Configuration file of S-switch-E

```
#
sysname S-switch-E
#
vlan batch 2
#
cfm enable
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 2
#
cfm md md1 level 6
ma ma1
map vlan 2
mep mep-id 3 interface GigabitEthernet 0/0/1 inward
mep ccm-send mep-id 3 enable
remote-mep mep-id 1
remote-mep ccm-receive mep-id 1 enable
remote-mep mep-id 2
remote-mep ccm-receive mep-id 2 enable
#
return
```

- Configuration file of S-switch-F

```
#
sysname S-switch-F
#
vlan batch 2 to 3
#
cfm enable
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 2 to 3
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 3
#
cfm md md1 level 6
ma ma1
map vlan 2
```

```

 ma ma2
 map vlan 3
 #
 return

```

- Configuration file of S-switch-G

```

#
sysname S-switch-G
#
vlan batch 3
#
cfm enable
#
interface GigabitEthernet0/0/3
 port trunk allow-pass vlan 3
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 3
#
cfm md mdl level 6
 ma ma2
 map vlan 3
 mep mep-id 2 interface GigabitEthernet 0/0/3 inward
 mep ccm-send mep-id 2 enable
 remote-mep mep-id 1
 remote-mep ccm-receive mep-id 1 enable
#
return

```

- Configuration file of S-switch-H

```

#
sysname S-switch-H
#
vlan batch 2 to 3
#
cfm enable
#
interface GigabitEthernet0/0/3
 port trunk allow-pass vlan 2 to 3
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 3
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 2
#
cfm md mdl level 6
 ma ma1
 map vlan 2
 mep mep-id 2 interface GigabitEthernet 0/0/2 inward
 mep ccm-send mep-id 2 enable
 remote-mep mep-id 1
 remote-mep ccm-receive mep-id 1 enable
 remote-mep mep-id 3
 remote-mep ccm-receive mep-id 3 enable
 ma ma2
 map vlan 3
 mep mep-id 1 interface GigabitEthernet 0/0/1 inward
 mep ccm-send mep-id 1 enable
 remote-mep mep-id 2
 remote-mep ccm-receive mep-id 2 enable
#
return

```

- Configuration file of S-switch-I

```

#
sysname S-switch-I
#
vlan batch 2
#

```

```
cfm enable
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 2
#
cfm md mdl level 6
ma ma1
map vlan 2
mep mep-id 1 interface GigabitEthernet 0/0/1 inward
mep ccm-send mep-id 1 enable
remote-mep mep-id 2
remote-mep ccm-receive mep-id 2 enable
remote-mep mep-id 3
remote-mep ccm-receive mep-id 3 enable
#
return
```



# 2 BFD Configuration

---

## About This Chapter

This chapter describes the basic principle of BFD, configurations of basic functions, and provides configuration examples.

### [2.1 Introduction](#)

This section describes the concept and the application of BFD.

### [2.2 Configuring the Single-Hop BFD](#)

This section describes how to configure the single-hop BFD.

### [2.3 Configuring the Multi-Hop BFD](#)

This section describes how to configure the multi-hop BFD.

### [2.4 Associating the BFD Session Status with the Interface Status](#)

This section describes how to associate the BFD session status with the interface status.

### [2.5 Adjusting BFD Detection Parameters](#)

This section describes how to adjust BFD parameters.

### [2.6 Maintaining BFD](#)

This section describes how to clear the BFD statistics and debug BFD.

### [2.7 Configuration Examples](#)

This section provides several configuration examples of BFD.

## 2.1 Introduction

This section describes the concept and the application of BFD.

### 2.1.1 BFD Overview

#### 2.1.2 BFD Features Supported by the S-switch

#### 2.1.3 Logical Relationships Between Configuration Tasks

#### 2.1.4 Update History

### 2.1.1 BFD Overview

The Bidirectional Forwarding Detection (BFD) is a unified detection mechanism of the entire network to detect communication faults of forwarding devices. BFD detects the connectivity of a type of data protocol, such as the IP protocol, between two devices or on the same path.

The BFD provides the following functions:

- Provides low-load and short-duration detection for path faults between adjacent forwarding devices.
- Uses a single mechanism to perform real-time detection for all media or protocol layers and supports different detection time and costs.

### 2.1.2 BFD Features Supported by the S-switch

This section introduces BFD features supported by the S-switch.

The S-switch send BFD control packets according to the negotiated period. If a S-switch does not receive the packet of the peer within the detection time, the BFD session becomes Down. The upper-layer applications can take the action according to the status of the BFD session.

### Single-Hop BFD

"Hop" refers to one hop on the IP network. The single-hop BFD is used to detect the connectivity of the forwarding link between two directly connected devices.

In the two systems detected by single-hop BFD, only one BFD session exists on the specified interface for a specified data protocol. Therefore, the BFD session is bound to the interface. On the S-switch, a BFD session can be bound to a Layer 2 physical interface, an Eth-Trunk member interface, a GE interface, or a Layer 3 VLANIF interface.

### Multi-Hop BFD

The multi-hop BFD is used to detect IP connectivity of any path between two non-directly-connected devices. These paths may span many hops or overlap. The multi-hop BFD is used to detect whether a reachable route exists between two devices.

The S-switch provides the multi-hop BFD for static routes. Generally, static routes do not have the detection mechanism. When the network fails, administrator interference is required. You can use the multi-hop BFD to check the status of static routes. The route management (RM)

module determines whether the static route is available or not according to the status of the BFD session.

## Dynamically Changing BFD Parameters

After a BFD session is set up, you can change the following parameters of BFD:

- Expected interval for sending BFD packets
- Minimum interval for receiving BFD packets
- Local detection time multiplier

This does not affect the status of the BFD session.

### 2.1.3 Logical Relationships Between Configuration Tasks

| If you want to...                                          | Then Perform the Task of...                                                                                                                                                                        |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Detect the connectivity of directly connected links        | <a href="#">2.2 Configuring the Single-Hop BFD</a>                                                                                                                                                 |
| Detect the connectivity of IP routing between S-switches   | <a href="#">2.3 Configuring the Multi-Hop BFD</a>                                                                                                                                                  |
| Associate the BFD session status with the interface status | <ul style="list-style-type: none"> <li>• <a href="#">2.2 Configuring the Single-Hop BFD</a></li> <li>• <a href="#">2.4 Associating the BFD Session Status with the Interface Status</a></li> </ul> |

### 2.1.4 Update History

| Version         | Revision                   |
|-----------------|----------------------------|
| V200R002C01B010 | This is the first release. |

## 2.2 Configuring the Single-Hop BFD

This section describes how to configure the single-hop BFD.

[2.2.1 Establishing the Configuration Task](#)

[2.2.2 Enabling Global BFD](#)

[2.2.3 \(Optional\) Setting the Default Multicast IP Address](#)

[2.2.4 Creating a BFD Session](#)

[2.2.5 \(Optional\) Configuring Descriptions of the BFD Session](#)

[2.2.6 Checking the Configuration](#)

## 2.2.1 Establishing the Configuration Task

### Applicable Environment

To fast detect and monitor the directly connected links on the network, configure the single-hop BFD.

### Pre-configuration Tasks

Before configuring the single-hop BFD, complete the following tasks:

- Connecting interfaces and setting physical parameters of the interface to turn the interface at the physical layer to Up
- Assigning an IP address to the Layer 3 interface correctly (On the S-switch, the Layer 3 interface refers to the VLANIF interface)

### Data Preparation

To configure the single-hop BFD, you need the following data.

| No. | Data                                                                                                                                                  |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Configuration name of the BFD session                                                                                                                 |
| 2   | Default multicast address, local interface name, and interface number<br>Or, the peer IP address for detecting the status of Layer 3 forwarding links |
| 3   | BFD session parameters: local and remote discriminators                                                                                               |

## 2.2.2 Enabling Global BFD

### Context

Do as follows on the S-switchs at both ends of the link to be detected.

### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **bfd** command to enable global BFD and enter the BFD view.

By default, global BFD is disabled. Before configuring BFD, you must enable global BFD; otherwise, the configuration fails.

----End

## 2.2.3 (Optional) Setting the Default Multicast IP Address

## Context

Do as follows on the S-switchs at both ends of the link to be detected.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bfd** command to enter the BFD view.
- Step 3** Run the **default-ip-address ip-address** command to set the default multicast IP address of the BFD session.

To perform the single-hop BFD for Layer 2 forwarding links, you need use the multicast IP address. By default, BFD uses the multicast IP address 224.0.0.184.

### NOTE

If the default multicast IP address is used for other protocols on the network, you must change the default multicast IP address.

The S-switchs at both ends of a BFD session must use the same multicast IP address.

----End

## 2.2.4 Creating a BFD Session

### Context

Do as follows on the S-switchs at both ends of the link to be detected.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bfd configuration-name bind peer-ip default-ip interface interface-type interface-number** command to create a BFD session to detect Layer 2 forwarding links, or the **bfd configuration-name bind peer-ip peer-ip interface interface-type interface-number** command to create a BFD session to detect Layer 3 forwarding links.

- Step 3** Set the discriminators.

- Run the **discriminator local discriminator** command to set the local discriminator.
- Run the **discriminator remote discriminator** command to set the remote discriminator.

When the discriminators are set, the local discriminator at the local end must be the same as the remote discriminator at the peer end; otherwise, the BFD session fails to be set up.

### NOTE

For the BFD session to which the default multicast IP address is bound, the local and remote discriminators of the BFD session cannot be the same.

- Step 4** Run the **commit** command to commit the configuration.

----End

## 2.2.5 (Optional) Configuring Descriptions of the BFD Session

## Context

Do as follows on the S-switchs at both ends of the link to be detected.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bfd configuration-name** command to enter the BFD session view.
- Step 3** Run the **description description** command to configure the descriptions of the BFD session.
- By default, the descriptions of a BFD session are null.
- Step 4** Run the **commit** command to commit the configuration.
- End

## 2.2.6 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                 | Command                                                                                                                                                                                                                  |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Check the BFD configuration.           | <b>display bfd configuration</b> { <b>all</b>   <b>static</b> [ <b>name</b> <i>cfg-name</i> ]   <b>dynamic</b>   <b>peer-ip</b> <i>peer-ip</i> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] } [ <b>verbose</b> ]     |
| Check the BFD interface.               | <b>display bfd interface</b> [ <i>interface-type interface-number</i> ]                                                                                                                                                  |
| Check the BFD session.                 | <b>display bfd session</b> { <b>all</b>   <b>static</b>   <b>dynamic</b>   <b>discriminator</b> <i>discr-value</i>   <b>peer-ip</b> <i>peer-ip</i> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] } [ <b>verbose</b> ] |
| Check the statistics of a BFD session. | <b>display bfd statistics session</b> { <b>all</b>   <b>static</b>   <b>dynamic</b>   <b>discriminator</b> <i>discr-value</i>   <b>peer-ip</b> <i>peer-ip</i> }                                                          |

Run the **display bfd configuration** command, and you can view the configuration of the BFD session.

```
<Quidway> display bfd configuration static name t verbose

BFD Session Configuration Name : t

Local Discriminator : 30 Remote Discriminator : 30
BFD Bind Type : Interface(Vlanif1)
Bind Session Type : Static
Bind Peer Ip Address : 1.1.1.1
Bind Interface : Vlanif1
Bind Source Ip Address : 1.1.1.2
TOS-EXP : 6
Min Tx Interval (ms) : 1000
Proc interface status : Disable
Local Demand Mode : Disable
Bind Application : No Application Bind
Session Description : 2

```

Run the **display bfd interface** command, and you can view information about the BFD session on the specified interface.

```
<Quidway> display bfd interface vlanif 1
```

| Interface Name | MIndex | Sess-Count | BFD-State |
|----------------|--------|------------|-----------|
| Vlanif1        | 1024   | 2          | up        |

Run the **display bfd session** command, and you can view information about the BFD session.

```
<Quidway> display bfd session all
```

| Local | Remote | Peer IP Address | Interface Name       | State | Type   |
|-------|--------|-----------------|----------------------|-------|--------|
| 1     | 2      | 1.1.1.1         | Vlanif1              | Down  | Static |
| 20    | 21     | 224.0.0.184     | GigabitEthernet0/0/1 | Down  | Static |
| 50    | 51     | 224.0.0.184     | GigabitEthernet0/0/1 | Down  | Static |
| 30    | 30     | 1.1.1.1         | Vlanif1              | Down  | Static |

Run the **display bfd statistics session** command, and you can view the statistics of the BFD session.

```
<Quidway> display bfd statistics session peer-ip 1.1.1.1
```

|                            |                       |              |             |
|----------------------------|-----------------------|--------------|-------------|
| Session MIndex : 4096      | (One Hop)             | State : Down | Name : test |
| Session Type               | : Static              |              |             |
| Local/Remote Discriminator | : 1/2                 |              |             |
| Received Packets           | : 0                   |              |             |
| Send Packets               | : 30799               |              |             |
| Received Bad Packets       | : 0                   |              |             |
| Send Bad Packets           | : 3                   |              |             |
| Down Count                 | : 0                   |              |             |
| ShortBreak Count           | : 0                   |              |             |
| Create Time                | : 2008/00/06 21:37:51 |              |             |
| Last Down Time             | : 0000/00/00 00:00:00 |              |             |
| Down Status Lasting Time   | : 000D:19H:41M:27S    |              |             |
| Total Time From Create     | : 000D:19H:41M:27S    |              |             |

Total Session Number : 2

## 2.3 Configuring the Multi-Hop BFD

This section describes how to configure the multi-hop BFD.

### 2.3.1 Establishing the Configuration Task

### 2.3.2 Enabling Global BFD

### 2.3.3 Creating a BFD Session

### 2.3.4 (Optional) Configuring Descriptions of the BFD Session

### 2.3.5 Checking the Configuration

## 2.3.1 Establishing the Configuration Task

### Applicable Environment

To fast detect and monitor the connectivity of IP routes between the S-switchs, configure the multi-hop BFD.

### Pre-configuration Tasks

Before configuring the multi-hop BFD, complete the following tasks:

- Connecting interfaces and setting physical parameters of the interface to turn the interface at the physical layer to Up
- Setting the link layer protocol parameters and IP address for the interface to turn the interface at the link protocol to Up
- Configuring the routing protocol to make the IP routes between the nodes reachable

### Data Preparation

To configure the multi-hop BFD, you need the following data.

| No. | Data                                                    |
|-----|---------------------------------------------------------|
| 1   | IP address of the peer device                           |
| 2   | Configuration name of the BFD session                   |
| 3   | BFD session parameters: local and remote discriminators |

## 2.3.2 Enabling Global BFD

### Context

Do as follows on the S-switchs at both ends of the link to be detected.

### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **bfd** command to enable global BFD.

By default, global BFD is disabled. Before configuring the BFD, you must enable global BFD; otherwise, the configuration fails.

----End

## 2.3.3 Creating a BFD Session

## Context

Do as follows on the S-switchs at both ends of the link to be detected.

## Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **bfd configuration-name bind peer-ip peer-ip [ source-ip source-ip ]** command to create a BFD session to detect Layer 3 forwarding links.

**Step 3** Set the discriminators.

- Run the **discriminator local discriminator** command to set the local discriminator.
- Run the **discriminator remote discriminator** command to set the remote discriminator.

When the discriminators are set, the local discriminator at the local end must be the same as the remote discriminator at the remote end; otherwise, the BFD session fails to be set up.

**Step 4** Run the **commit** command to commit the configuration.

----End

## 2.3.4 (Optional) Configuring Descriptions of the BFD Session

## Context

Do as follows on the S-switchs at both ends of the link to be detected.

## Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **bfd configuration-name** command to enter the BFD session view.

**Step 3** Run the **description description** command to configure the descriptions of the BFD session.

By default, the descriptions of a BFD session are null.

**Step 4** Run the **commit** command to commit the configuration.

----End

## 2.3.5 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                       | Command                                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Check the BFD configuration. | <b>display bfd configuration { all   static [ name cfg-name ]   dynamic   peer-ip peer-ip [ vpn-instance vpn-instance-name ] } [ verbose ]</b> |

| Action                                   | Command                                                                                                                                                                                                                  |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Check the BFD session.                   | <b>display bfd session</b> { <b>all</b>   <b>static</b>   <b>dynamic</b>   <b>discriminator</b> <i>discr-value</i>   <b>peer-ip</b> <i>peer-ip</i> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] } [ <b>verbose</b> ] |
| Check the statistics of the BFD session. | <b>display bfd statistics session</b> { <b>all</b>   <b>static</b>   <b>dynamic</b>   <b>discriminator</b> <i>discr-value</i>   <b>peer-ip</b> <i>peer-ip</i> }                                                          |

Run the **display bfd configuration** command, and you can view the configuration of the BFD session.

```
<Quidway> display bfd configuration static name t1 verbose

BFD Session Configuration Name : t1

Local Discriminator : 40 Remote Discriminator : 40
BFD Bind Type : Peer Ip Address
Bind Session Type : Static
Bind Peer Ip Address : 1.1.1.1
Bind Interface : --
Bind Source Ip Address : 1.1.1.2
TOS-EXP : 6 Local Detect Multi : 3
Min Tx Interval (ms) : 1000 Min Rx Interval (ms) : 1000
Proc interface status : Disable WTR Interval (ms) : --
Local Demand Mode : Disable
Bind Application : No Application Bind
Session Description : --

```

Run the **display bfd session** command, and you can view information about the BFD session.

```
<Quidway> display bfd session discriminator 40 verbose

Session MIndex : 4100 (Multi Hop) State : Down Name : t1

Local Discriminator : 40 Remote Discriminator : 40
Session Detect Mode : Asynchronous Mode Without Echo Function
BFD Bind Type : Peer Ip Address
Bind Session Type : Static
Bind Peer Ip Address : 1.1.1.1
Bind Interface : --
Bind Source Ip Address : 1.1.1.2
FSM Board Id : 0 TOS-EXP : 6
Min Tx Interval (ms) : 1000 Min Rx Interval (ms) : 1000
Actual Tx Interval (ms) : 2300 Actual Rx Interval (ms) : 2300
Local Detect Multi : 3 Detect Interval (ms) : --
Echo Passive : Disable Acl Number : --
Proc interface status : Disable
WTR Interval (ms) : -- Local Demand Mode : Disable
Last Local Diagnostic : No Diagnostic
Bind Application : No Application Bind
Session TX TmrID : 1032 Session Detect TmrID : --
Session Init TmrID : -- Session WTR TmrID : --
Session Echo Tx TmrID : --
PDT Index : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description : --

```

Run the **display bfd statistics session** command, and you can view the statistics of the BFD session.

```
<Quidway> display bfd statistics session all

Session MIndex : 4100 (Multi Hop) State : Down Name : t1

```

```

Session Type : Static
Local/Remote Discriminator : 40/40
Received Packets : 0
Send Packets : 138
Received Bad Packets : 0
Send Bad Packets : 147
Down Count : 0
ShortBreak Count : 0
Create Time : 2008/00/07 17:37:45
Last Down Time : 0000/00/00 00:00:00
Down Status Lasting Time : 000D:00H:11M:05S
Total Time From Create : 000D:00H:11M:05S

```

## 2.4 Associating the BFD Session Status with the Interface Status

This section describes how to associate the BFD session status with the interface status.

### [2.4.1 Establishing the Configuration Task](#)

### [2.4.2 Associating the BFD Session Status with the Interface Status](#)

### [2.4.3 Checking the Configuration](#)

## 2.4.1 Establishing the Configuration Task

### Applicable Environment

When the BFD session detects faults and becomes Down, the interface becomes Down, if the BFD session status is associated with the interface status. In this case, the direct route of the interface is deleted from the routing table. BFD packets, however, can still be sent.

### Pre-configuration Tasks

Before associating the BFD session status with the interface status, complete the following task:

- [2.2 Configuring the Single-Hop BFD](#)

#### NOTE

To associate the BFD session status with the interface status, you must use the single-hop BFD session bound to the default multicast IP address.

### Data Preparation

To associate the BFD status with the sub-interface status, you need the following data.

| No. | Data                    |
|-----|-------------------------|
| 1   | Name of the BFD session |

## 2.4.2 Associating the BFD Session Status with the Interface Status

### Context

Do as follows on the S-switchs where the BFD session status needs to be associated with the interface status.

### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **bfd configuration-name** command to enter the BFD session view.

**Step 3** Run the **process-interface-status** command to associate the DFD session status with the interface status.

By default, the BFD session status is not associated with the interface status. That is, the change of the BFD session status does not affect the interface status.

#### NOTE

The BFD session status can be associated with the interface status only after the BFD session status is Up.

**Step 4** Run the **commit** command to commit the configuration.

----End

## 2.4.3 Checking the Configuration

Run the following command to check the previous configuration.

| Action                                   | Command                                                                                                                                                    |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Check information about the BFD session. | <b>display bfd session { all   static   dynamic   discriminator discriminator-value   peer-ip peer-ip [ vpn-instance vpn-instance-name ] } [ verbose ]</b> |

# Run the **display bfd session** command, and you can view information about the BFD session.

```
<Quidway> display bfd session all verbose
Total Static Session Number : 5, Dynamic Session Number: 0

Session MIndex : 4096 (One Hop) State : Down Name : test

Local Discriminator : 1 Remote Discriminator : 2
Session Detect Mode : Asynchronous Mode Without Echo Function
BFD Bind Type : Interface(Vlanif1)
Bind Session Type : Static
Bind Peer Ip Address : 1.1.1.1
Bind Interface : Vlanif1
Bind Source Ip Address : 1.1.1.2
FSM Board Id : 0
Min Tx Interval (ms) : 1000 TOS-EXP : 6
Actual Tx Interval (ms) : 2300 Min Rx Interval (ms) : 1000
Local Detect Multi : 3 Actual Rx Interval (ms) : 2300
Echo Passive : Disable Detect Interval (ms) : --
Proc interface status : Enable Acl Number : --
WTR Interval (ms) : -- Local Demand Mode : Disable
Last Local Diagnostic : No Diagnostic
```

```

Bind Application : No Application Bind
Session TX TmrID : 1028 Session Detect TmrID : --
Session Init TmrID : -- Session WTR TmrID : --
Session Echo Tx TmrID : --
PDT Index : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description : --

Session MIndex : 4097 (One Hop) State : Down Name : test1

Local Discriminator : 20 Remote Discriminator : 21
Session Detect Mode : Asynchronous Mode Without Echo Function
BFD Bind Type : Interface(GigabitEthernet0/0/1)
Bind Session Type : Static
Bind Peer Ip Address : 224.0.0.184
Bind Interface : GigabitEthernet0/0/1
Bind Source Ip Address : 1.1.1.2
FSM Board Id : 0 TOS-EXP : 6
Min Tx Interval (ms) : 1000 Min Rx Interval (ms) : 1000
Actual Tx Interval (ms) : 2400 Actual Rx Interval (ms): 2400
Local Detect Multi : 3 Detect Interval (ms) : --
Echo Passive : Disable Acl Number : --
Proc interface status : Enable
WTR Interval (ms) : -- Local Demand Mode : Disable
Last Local Diagnostic : No Diagnostic
Bind Application : No Application Bind
Session TX TmrID : 1029 Session Detect TmrID : --
Session Init TmrID : -- Session WTR TmrID : --
Session Echo Tx TmrID : --
PDT Index : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description : --

Session MIndex : 4098 (One Hop) State : Down Name : test0

Local Discriminator : 50 Remote Discriminator : 51
Session Detect Mode : Asynchronous Mode Without Echo Function
BFD Bind Type : Interface(GigabitEthernet0/0/1)
Bind Session Type : Static
Bind Peer Ip Address : 224.0.0.184
Bind Interface : GigabitEthernet0/0/1
Bind Source Ip Address : 1.1.1.2
FSM Board Id : 0 TOS-EXP : 6
Min Tx Interval (ms) : 1000 Min Rx Interval (ms) : 1000
Actual Tx Interval (ms) : 2600 Actual Rx Interval (ms): 2600
Local Detect Multi : 3 Detect Interval (ms) : --
Echo Passive : Disable Acl Number : --
Proc interface status : Enable
WTR Interval (ms) : -- Local Demand Mode : Disable
Last Local Diagnostic : No Diagnostic
Bind Application : No Application Bind
Session TX TmrID : 1030 Session Detect TmrID : --
Session Init TmrID : -- Session WTR TmrID : --
Session Echo Tx TmrID : --
PDT Index : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description : --

Session MIndex : 4099 (One Hop) State : Down Name : t

Local Discriminator : 30 Remote Discriminator : 30
Session Detect Mode : Asynchronous Mode Without Echo Function
BFD Bind Type : Interface(Vlanif1)
Bind Session Type : Static
Bind Peer Ip Address : 1.1.1.1
Bind Interface : Vlanif1

```

```

Bind Source Ip Address : 1.1.1.2
FSM Board Id : 0
Min Tx Interval (ms) : 1000
Actual Tx Interval (ms): 2400
Local Detect Multi : 3
Echo Passive : Disable
Proc interface status : Enable
WTR Interval (ms) : --
Last Local Diagnostic : No Diagnostic
Bind Application : No Application Bind
Session TX TmrID : 1031
Session Init TmrID : --
Session Echo Tx TmrID : --
PDT Index : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description : 2
TOS-EXP : 6
Min Rx Interval (ms) : 1000
Actual Rx Interval (ms): 2400
Detect Interval (ms) : --
Acl Number : --
Local Demand Mode : Disable
Session Detect TmrID : --
Session WTR TmrID : --

Session MIndex : 4100 (Multi Hop) State : Down Name : t1

Local Discriminator : 40
Remote Discriminator : 40
Session Detect Mode : Asynchronous Mode Without Echo Function
BFD Bind Type : Peer Ip Address
Bind Session Type : Static
Bind Peer Ip Address : 1.1.1.1
Bind Interface : --
Bind Source Ip Address : 1.1.1.2
FSM Board Id : 0
Min Tx Interval (ms) : 1000
Actual Tx Interval (ms) : 2300
Local Detect Multi : 3
Echo Passive : Disable
Proc interface status : Enable
WTR Interval (ms) : --
Last Local Diagnostic : No Diagnostic
Bind Application : No Application Bind
Session TX TmrID : 1032
Session Init TmrID : --
Session Echo Tx TmrID : --
PDT Index : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description : --
TOS-EXP : 6
Min Rx Interval (ms) : 1000
Actual Rx Interval (ms) : 2300
Detect Interval (ms) : --
Acl Number : --
Local Demand Mode : Disable
Session Detect TmrID : --
Session WTR TmrID : --

```

## 2.5 Adjusting BFD Detection Parameters

This section describes how to adjust BFD parameters.

### [2.5.1 Establishing the Configuration Task](#)

### [2.5.2 Adjusting the BFD Detection Time](#)

### [2.5.3 Setting the WTR for a BFD Session](#)

### [2.5.4 Setting the Priority of BFD Packets](#)

### [2.5.5 Checking the Configuration](#)

## 2.5.1 Establishing the Configuration Task

### Applicable Environment

When setting up a BFD session, you can adjust the following parameters as required:

- Expected interval for sending BFD packets

- Minimum interval for receiving BFD packets
- Local detection time multiplier

You can set the Wait to Restore (WTR) for a BFD session to avoid frequent status switchover of upper layer applications caused by the BFD session flapping.

Generally, the default configuration is used.

## Pre-configuration Tasks

Before adjusting BFD detection parameters, complete the following task:

- Creating a BFD session

## Data Preparation

To adjust BFD detection parameters, you need the following data.

| No. | Data                                                                                     |
|-----|------------------------------------------------------------------------------------------|
| 1   | Configuration name of the BFD session                                                    |
| 2   | Expected interval for sending BFD packets and minimum interval for receiving BFD packets |
| 3   | Local detection time multiplier for BFD packets                                          |
| 4   | Priorities of BFD packets                                                                |

## 2.5.2 Adjusting the BFD Detection Time

### Context

To reduce the usage of system resources, when a BFD session is detected in the Down state, the system adjusts the intervals for sending and receiving BFD packets at the local end to a random value from 1000 to 3000. When the BFD session becomes Up, the set interval is restored.

Do as follows on the S-switchs that need adjust BFD parameters:

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bfd configuration-name** command to enter the BFD session view.
- Step 3** Run the **min-tx-interval interval** command to set the expected interval for sending BFD packets.

The value is an integer that ranges from 200 to 1000, in milliseconds(ms). By default, the value is 1000 milliseconds.

When configuring the multi-hop BFD, you cannot modify the expected interval for sending BFD packets. At the moment, the expected interval for sending BFD packets is 1000 milliseconds.

**Step 4** Run the **min-rx-interval** *interval* command to set the minimum interval for receiving BFD packets.

The value is an integer that ranges from 200 to 1000, in milliseconds(ms). By default, the value is 1000 milliseconds.

When configuring the multi-hop BFD, you cannot modify the minimum interval for receiving BFD packets. At the moment, the minimum interval for receiving BFD packets is 1000 milliseconds.

**Step 5** Run the **detect-multiplier** *multiplier* command to set the local detection time multiplier.

By default, the local detection time multiplier is 3.

**Step 6** Run the **commit** command to commit the configuration.

----End

## 2.5.3 Setting the WTR for a BFD Session

### Context

The instability of a network results in frequent status changes of a BFD session. This causes frequent status changes of upper-layer applications. The upper-layer applications, however, take the action according to the status of the BFD session.

To avoid the problem, you can set the WTR for a BFD session. When the BFD session changes from Down to Up, the BFD reports the change to the upper-layer applications after the WTR expires. When the BFD session changes from Up to Down, the BFD still reports the change to the upper-layer applications immediately.

Do as follows on the S-switches that need adjust BFD parameters:

### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **bfd configuration-name** command to enter the BFD session view.

**Step 3** Run the **wtr wtr** command to set the WTR.

By default, the WTR is 0, that is, the device does not wait to restore.

#### NOTE

A BFD session is unidirectional. If the WTR is set, you need set the same WTR at both ends. Otherwise, when the session status changes at one end, the BFD session status sensed by the applications at both ends is different.

**Step 4** Run the **commit** command to commit the configuration.

----End

## 2.5.4 Setting the Priority of BFD Packets

## Context

You can change the priority of BFD packets to:

- Detect whether packets of different priorities on the same link can be forwarded.
- Ensure that BFD packets with high priorities are forwarded first.

Do as follows on the S-switchs that need adjust BFD parameters:

## Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **bfd configuration-name** command to enter the BFD session view.

**Step 3** Run the **tos-exp tos** command to set the priority of BFD packets.

The lowest priority is 0 and the highest priority is 6. By default, the priority of BFD packets is 6.

**Step 4** Run the **commit** command to commit the configuration.

----End

## 2.5.5 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                       | Command                                                                                                                                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Check the BFD configuration. | <b>display bfd configuration</b> { <b>all</b>   <b>static</b> } [ <b>for-ip</b> ] [ <b>verbose</b> ]<br><b>display bfd configuration</b> { <b>static</b> [ <b>name configuration-name</b> ]   <b>peer-ip peer-ip</b> } [ <b>verbose</b> ] |
| Check the BFD session.       | <b>display bfd session</b> { <b>all</b>   <b>static</b> } [ <b>for-ip</b> ] [ <b>verbose</b> ]<br><b>display bfd session</b> { <b>discriminator discriminator</b>   <b>peer-ip peer-ip</b> } [ <b>verbose</b> ]                           |

Run the **display bfd configuration** command, and you can view the configuration of the BFD session.

```
<Quidway> display bfd configuration static name t1 verbose
```

```

BFD Session Configuration Name : t1

Local Discriminator : 40 Remote Discriminator : 40
BFD Bind Type : Peer Ip Address
Bind Session Type : Static
Bind Peer Ip Address : 1.1.1.1
Bind Interface : --
Bind Source Ip Address : 1.1.1.2
TOS-EXP : 3 Local Detect Multi : 5
Min Tx Interval (ms) : 200 Min Rx Interval (ms) : 200
Proc interface status : Disable WTR Interval (ms) : 60000
Local Demand Mode : Disable
Bind Application : No Application Bind
Session Description : --

```

Run the **display bfd session** command, and you can view information about the BFD session.

<Quidway> **display bfd session all verbose**

Total Static Session Number : 5, Dynamic Session Number: 0

```

Session MIndex : 4096 (One Hop) State : Down Name : test

Local Discriminator : 1 Remote Discriminator : 2
Session Detect Mode : Asynchronous Mode Without Echo Function
BFD Bind Type : Interface(Vlanif1)
Bind Session Type : Static
Bind Peer Ip Address : 1.1.1.1
Bind Interface : Vlanif1
Bind Source Ip Address : 1.1.1.2
FSM Board Id : 0 TOS-EXP : 6
Min Tx Interval (ms) : 1000 Min Rx Interval (ms) : 1000
Actual Tx Interval (ms) : 2300 Actual Rx Interval (ms): 2300
Local Detect Multi : 3 Detect Interval (ms) : --
Echo Passive : Disable Acl Number : --
Proc interface status : Disable
WTR Interval (ms) : -- Local Demand Mode : Disable
Last Local Diagnostic : No Diagnostic
Bind Application : No Application Bind
Session TX TmrID : 1028 Session Detect TmrID : --
Session Init TmrID : -- Session WTR TmrID : --
Session Echo Tx TmrID : --
PDT Index : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description : --

```

```

Session MIndex : 4097 (One Hop) State : Down Name : test1

Local Discriminator : 20 Remote Discriminator : 21
Session Detect Mode : Asynchronous Mode Without Echo Function
BFD Bind Type : Interface(GigabitEthernet0/0/1)
Bind Session Type : Static
Bind Peer Ip Address : 224.0.0.184
Bind Interface : GigabitEthernet0/0/1
Bind Source Ip Address : 1.1.1.2
FSM Board Id : 0 TOS-EXP : 6
Min Tx Interval (ms) : 1000 Min Rx Interval (ms) : 1000
Actual Tx Interval (ms) : 2400 Actual Rx Interval (ms): 2400
Local Detect Multi : 3 Detect Interval (ms) : --
Echo Passive : Disable Acl Number : --
Proc interface status : Disable
WTR Interval (ms) : -- Local Demand Mode : Disable
Last Local Diagnostic : No Diagnostic
Bind Application : No Application Bind
Session TX TmrID : 1029 Session Detect TmrID : --
Session Init TmrID : -- Session WTR TmrID : --
Session Echo Tx TmrID : --
PDT Index : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description : --

```

```

Session MIndex : 4098 (One Hop) State : Down Name : test0

Local Discriminator : 50 Remote Discriminator : 51
Session Detect Mode : Asynchronous Mode Without Echo Function
BFD Bind Type : Interface(GigabitEthernet0/0/1)
Bind Session Type : Static
Bind Peer Ip Address : 224.0.0.184
Bind Interface : GigabitEthernet0/0/1
Bind Source Ip Address : 1.1.1.2
FSM Board Id : 0 TOS-EXP : 6
Min Tx Interval (ms) : 1000 Min Rx Interval (ms) : 1000
Actual Tx Interval (ms) : 2600 Actual Rx Interval (ms): 2600
Local Detect Multi : 3 Detect Interval (ms) : --

```

```

Echo Passive : Disable Acl Number : --
Proc interface status : Disable
WTR Interval (ms) : -- Local Demand Mode : Disable
Last Local Diagnostic : No Diagnostic
Bind Application : No Application Bind
Session TX TmrID : 1030 Session Detect TmrID : --
Session Init TmrID : -- Session WTR TmrID : --
Session Echo Tx TmrID : --
PDT Index : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description : --

Session MIndex : 4099 (One Hop) State : Down Name : t

Local Discriminator : 30 Remote Discriminator : 30
Session Detect Mode : Asynchronous Mode Without Echo Function
BFD Bind Type : Interface(Vlanif1)
Bind Session Type : Static
Bind Peer Ip Address : 1.1.1.1
Bind Interface : Vlanif1
Bind Source Ip Address : 1.1.1.2
FSM Board Id : 0 TOS-EXP : 6
Min Tx Interval (ms) : 1000 Min Rx Interval (ms) : 1000
Actual Tx Interval (ms) : 2400 Actual Rx Interval (ms): 2400
Local Detect Multi : 3 Detect Interval (ms) : --
Echo Passive : Disable Acl Number : --
Proc interface status : Disable
WTR Interval (ms) : -- Local Demand Mode : Disable
Last Local Diagnostic : No Diagnostic
Bind Application : No Application Bind
Session TX TmrID : 1031 Session Detect TmrID : --
Session Init TmrID : -- Session WTR TmrID : --
Session Echo Tx TmrID : --
PDT Index : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description : 2

Session MIndex : 4100 (Multi Hop) State : Down Name : t1

Local Discriminator : 40 Remote Discriminator : 40
Session Detect Mode : Asynchronous Mode Without Echo Function
BFD Bind Type : Peer Ip Address
Bind Session Type : Static
Bind Peer Ip Address : 1.1.1.1
Bind Interface : --
Bind Source Ip Address : 1.1.1.2
FSM Board Id : 0 TOS-EXP : 3
Min Tx Interval (ms) : 200 Min Rx Interval (ms) : 200
Actual Tx Interval (ms) : 2300 Actual Rx Interval (ms): 2300
Local Detect Multi : 5 Detect Interval (ms) : --
Echo Passive : Disable Acl Number : --
Proc interface status : Disable
WTR Interval (ms) : 60000 Local Demand Mode : Disable
Last Local Diagnostic : No Diagnostic
Bind Application : No Application Bind
Session TX TmrID : 1032 Session Detect TmrID : --
Session Init TmrID : -- Session WTR TmrID : --
Session Echo Tx TmrID : --
PDT Index : FSM-0|RCV-0|IF-0|TOKEN-0
Session Description : --

```

## 2.6 Maintaining BFD

This section describes how to clear the BFD statistics and debug BFD.

[2.6.1 Clearing the BFD Statistics](#)[2.6.2 Debugging BFD](#)

## 2.6.1 Clearing the BFD Statistics

To clear the BFD statistics, run the following **reset** command in the user view.

| Action                    | Command                                                                                |
|---------------------------|----------------------------------------------------------------------------------------|
| Clear the BFD statistics. | <b>reset bfd statistics</b> { <b>all</b>   <b>discriminator</b> <i>discriminator</i> } |

## 2.6.2 Debugging BFD



### CAUTION

Debugging affects the performance of the system. So, after debugging, run the **undo debugging all** command to disable it immediately.

When a BFD fault occurs, run the following **debugging** command in the user view to locate and the fault.

| Action                           | Command                                                                                                                                                                                                                  |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable the BFD module debugging. | <b>debugging bfd</b> { <b>all</b>   <b>defect-detect</b>   <b>error</b>   <b>event</b>   <b>fsm</b>   <b>ha</b>   <b>packet</b>   <b>process</b>   <b>product-interface</b>   <b>session-management</b>   <b>timer</b> } |

## 2.7 Configuration Examples

This section provides several configuration examples of BFD.

[2.7.1 Example for Configuring the Single-Hop BFD](#)[2.7.2 Example for Configuring Multi-Hop BFD](#)

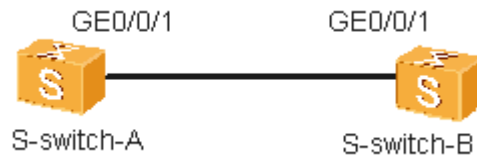
### 2.7.1 Example for Configuring the Single-Hop BFD

#### Networking Requirements

Interfaces on the S-switch are Layer 2 interfaces. To detect the connectivity of a Layer 2 forwarding link between the two directly connected S-switches, you can configure the single-hop BFD to bind a BFD session to the multicast IP address and the local interface.

As shown in **Figure 2-1**, a BFD session is set up to detect the connectivity of the Layer 2 link between S-switch-A and S-switch-B.

**Figure 2-1** Networking diagram of configuring the single-hop BFD for Layer 2 forwarding link



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a BFD session on S-switch-A to detect the directly connected link from S-switch-A to S-switch-B.
2. Configure a BFD session on S-switch-B to detect the directly connected link from S-switch-B to S-switch-A.

## Data Preparation

To complete the configuration, you need the following data:

- Type and number of the interface bound to the BFD session
- Local and remote discriminators of the BFD session

Default values of the minimum interval for sending BFD packets, the minimum interval for receiving BFD packets, and the detection time multiplier are used

## Configuration Procedure

1. Configure single-hop BFD on S-switch-A.

# Enable BFD on S-switch-A.

```
<Quidway> system-view
[Quidway] sysname S-switch-A
[S-switch-A] bfd
[S-switch-A-bfd] quit
```

# Set up a BFD session on S-switch-A.

```
[S-switch-A] bfd atob bind peer-ip default-ip interface gigabitethernet 0/0/1
[S-switch-A-bfd-session-atob] discriminator local 1
[S-switch-A-bfd-session-atob] discriminator remote 2
[S-switch-A-bfd-session-atob] commit
[S-switch-A-bfd-session-atob] quit
```

2. Configure single-hop BFD on S-switch-B.

# Enable BFD on S-switch-B.

```
<Quidway> system-view
[Quidway] sysname S-switch-B
[S-switch-B] bfd
[S-switch-B-bfd] quit
```

# Set up a BFD session on S-switch-B.

```
[S-switch-B] bfd btoa bind peer-ip default-ip interface gigabitethernet 0/0/1
[S-switch-B-bfd-session-btoa] discriminator local 2
```

```
[S-switch-B-bfd-session-btoa] discriminator remote 1
[S-switch-B-bfd-session-btoa] commit
[S-switch-B-bfd-session-btoa] quit
```

### 3. Verify the configuration.

After the configuration, run the **display bfd session** command on S-switch-A and S-switch-B, and you can find that a single-hop BFD session is set up and its status is Up.

Take the display on S-switch-A as an example.

```
<S-switch-A> display bfd session all verbose

--
Session MIndex : 4097 (One Hop) State : Up Name : atob

--
Local Discriminator : 1 Remote Discriminator : 2
Session Detect Mode : Asynchronous Mode Without Echo Function
BFD Bind Type : Interface(GigabitEthernet0/0/1)
Bind Session Type : Static
Bind Peer IP Address : 224.0.0.184
NextHop Ip Address : 224.0.0.184
Bind Interface : GigabitEthernet 0/0/2
FSM Board Id : 0 TOS-EXP : 6
Min Tx Interval (ms) : 1000 Min Rx Interval (ms) : 1000
Actual Tx Interval (ms) : 1000 Actual Rx Interval (ms): 1000
Local Detect Multi : 3 Detect Interval (ms) : 3000
Echo Passive : Disable Acl Number : -
WTR Interval (ms) : - WTR Timer State : Stop
Proc Interface Status : Disable Process PST : Disable
Active Multi : 3
Last Local Diagnostic : No Diagnostic
Bind Application : No Application Bind
Session TX TmrID : - Session Detect TmrID : -
Session Init TmrID : - Session WTR TmrID : -
Session Echo Tx TmrID : -
PDT Index : FSM-0 | RCV-0 | IF-0 | TOKEN-0
Session Description : -

--

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

## Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
bfd
#
bfd atob bind peer-ip default-ip interface GigabitEthernet0/0/1
discriminator local 1
discriminator remote 2
commit
#
return
```

- Configuration files of S-switch-B

```
#
sysname S-switch-B
#
bfd
#
bfd btoa bind peer-ip default-ip interface GigabitEthernet0/0/1
discriminator local 2
discriminator remote 1
commit
#
```

return

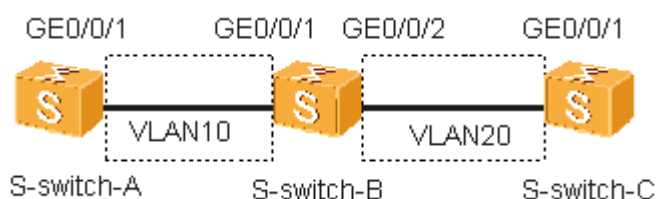
## 2.7.2 Example for Configuring Multi-Hop BFD

### Networking Requirements

As shown in **Figure 2-2**, the BFD session is set up to detect the multi-hop path from S-switch-A to S-switch-C.

Interfaces on the S-switch are Layer 2 interfaces. When configuring the multi-hop BFD, you need add an interface to a VLAN, create a VLANIF interface, and assign an IP address to the VLANIF interface.

**Figure 2-2** Networking diagram of configuring the multi-hop BFD



### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a BFD session on S-switch-A to detect the multi-hop path from S-switch-A to S-switch-C.
2. Configure a BFD session on S-switch-C to detect the multi-hop path from S-switch-C to S-switch-A.

### Data Preparation

To complete the configuration, you need the following data:

- Peer IP address bound to a BFD session
- Local and remote discriminators of a BFD session
- IP address of VLANIF 10 on S-switch-A being 10.1.1.0/16
- IP address of VLANIF 10 on S-switch-B being 10.1.1.0/16
- IP address of VLANIF 20 on S-switch-B being 10.2.1.0/16
- IP address of VLANIF 20 on S-switch-C being 10.2.1.0/16

Default values of the minimum interval for sending BFD control packets, the minimum interval for receiving BFD control packets, and the local detection time multiplier are used

### Configuration Procedure

1. Add an interface to the VLAN, create a VLANIF interface, and assign an IP address to the VLANIF interface.

# Create a VLAN on S-switch-A and add an interface to the VLAN.

```
<Quidway> system-view
```

```
[Quidway] sysname S-switch-A
[S-switch-A] vlan batch 10
[S-switch-A] interface gigabitethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[S-switch-A-GigabitEthernet0/0/1] quit
```

# Create a VLNAIF interface and assign an IP address to the VLANIF interface.

```
[S-switch-A] interface vlanif 10
[S-switch-A-Vlanif10] ip address 10.1.1.1 16
[S-switch-A-Vlanif10] quit
```

The configurations on S-switch-B and S-switch-C is the same as the configuration on S-switch-A, so the configuration details are not mentioned here.

2. Configure a static route so that there is a reachable route between S-switch-A and S-switch-C.

```
[S-switch-A] ip route-static 10.2.1.2 16 10.1.1.2
```

The configuration on S-switch-C is the same as that on S-switch-A, so the configuration details are not mentioned here.

3. Configure multi-hop BFD on S-switch-A and S-switch-C.

# On S-switch-A, set up a BFD session with S-switch-C.

```
<S-switch-A> system-view
[S-switch-A] bfd
[S-switch-A-bfd] quit
[S-switch-A] bfd atoc bind peer-ip 10.2.1.2
[S-switch-A-bfd-session-atoc] discriminator local 10
[S-switch-A-bfd-session-atoc] discriminator remote 20
[S-switch-A-bfd-session-atoc] commit
[S-switch-A-bfd-session-atoc] quit
```

# On S-switch-C, set up a BFD session with S-switch-A.

```
<S-switch-C> system-view
[S-switch-C] bfd
[S-switch-C-bfd] quit
[S-switch-C] bfd ctoa bind peer-ip 10.1.1.1
[S-switch-C-bfd-session-ctoa] discriminator local 20
[S-switch-C-bfd-session-ctoa] discriminator remote 10
[S-switch-C-bfd-session-ctoa] commit
[S-switch-C-bfd-session-ctoa] quit
```

4. Verify the configuration.

After the configuration, run the **display bfd session** command on S-switch-A and S-switch-C, and you can find that a BFD session is set up and its status is Up.

Take the display on S-switch-A as an example.

```
<S-switch-A> display bfd session all verbose
```

```

--
Session MIndex : 4096 (Multi Hop) State : Up Name : atoc

--
Local Discriminator : 10 Remote Discriminator : 20
Session Detect Mode : Asynchronous Mode Without Echo Function
BFD Bind Type : Peer IP Address
Bind Session Type : Static
Bind Peer IP Address : 10.2.1.2
Bind Interface : -
FSM Board Id : 0
Min Tx Interval (ms) : 1000 Min Rx Interval (ms) : 1000
Actual Tx Interval (ms) : 1000 Actual Rx Interval (ms) : 1000
Local Detect Multi : 3 Detect Interval (ms) : 3000
Echo Passive : Disable Acl Number : -
WTR Interval (ms) : 1800000 WTR Timer State : Stop
Proc Interface Status : Disable Process PST : Disable
Active Multi : 3
```

```

Last Local Diagnostic : Control Detection Time Expired
Bind Application : No Application Bind
Session TX TmrID : 16434 Session Detect TmrID : 16435
Session Init TmrID : - Session WTR TmrID : -
Session Echo Tx TmrID : -
PDT Index : FSM-0 | RCV-0 | IF-0 | TOKEN-0
Session Description : -

--

```

Total UP/DOWN Session Number : 0/0

## Configuration Files

- Configuration file of S-switch-A

```

#
sysname S-switch-A
#
bfd
#
interface Vlanif10
ip address 10.1.1.1 255.255.0.0
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
bfd atoc bind peer-ip 10.2.1.2
discriminator local 10
discriminator remote 20
commit
#
ip route-static 10.2.0.0 255.255.0.0 10.1.1.2
#
return

```

- Configuration files of S-switch-B

```

#
sysname S-switch-B
#
interface Vlanif10
ip address 10.1.1.2 255.255.0.0
#
interface Vlanif20
ip address 10.2.1.1 255.255.0.0
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 20
#
return

```

- Configuration files of S-switch-C

```

#
sysname S-switch-C
#
bfd
#
interface Vlanif20
ip address 10.2.1.2 255.255.0.0
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 20
#
bfd ctoa bind peer-ip 10.1.1.1
discriminator local 20
discriminator remote 10
commit

```

```

ip route-static 10.1.0.0 255.255.0.0 10.2.1.1

return
```

# 3 Smart Link Configuration

---

## About This Chapter

This chapter describes the implementation and configuration procedures of Smart Link on the S-switch.

### [3.1 Introduction](#)

This section briefly describes Smart Link, Monitor Link, the logical relationship between configuration tasks, and the difference between this version and the previous version.

### [3.2 Configuring Basic Functions of a Smart Link Group](#)

This section describes how to configure basic functions of a Smart Link group, such as to create a Smart Link group, enable the functions of the group, configure the master and slave interfaces, enable revertive switching, and configure Flush packets.

### [3.3 Configuring the Data Stream Policy of the Smart Link Group](#)

This section describes how to configure the advanced functions of the Smart Link group, such as to lock data streams and switch traffic between links manually.

### [3.4 Configuring Functions of a Monitor Link Group](#)

This section describes how to configure functions of a Monitor Link group, such as to create a Monitor Link group, configure uplink and downlink interfaces, and enable revertive switching.

### [3.5 Maintaining Smart Link](#)

This section describes how to debug Smart Link.

### [3.6 Configuration Examples](#)

This section provides several configuration examples of Smart Link.

## 3.1 Introduction

This section briefly describes Smart Link, Monitor Link, the logical relationship between configuration tasks, and the difference between this version and the previous version.

### [3.1.1 Smart Link and Monitor Link](#)

### [3.1.2 Logical Relationships Between Configuration Tasks](#)

#### 3.1.1 Smart Link and Monitor Link

Smart Link provides a solution to the link backup and rapid switching between the active link and standby link in dual-homed networking. The redundant link is blocked to provide backup for the link in the dual-homed uplink networking environment. When the active link fails, the traffic is switched to the standby link.

Monitor Link is introduced as a supplement to Smart Link. This technology supports the association of interfaces. A Monitor Link group consists of an uplink interface and multiple downlink interfaces. If the uplink interface fails, the Monitor Link group automatically shuts down the downlink interfaces. The downlink interfaces also recover along with the uplink interface.

#### 3.1.2 Logical Relationships Between Configuration Tasks

You must configure the basic functions of the Smart Link group before configuring the data stream policy. The data stream policy can be configured only when the Smart Link group has the basic functions.

You must configure Smart Link before configuring Monitor Link. As a supplement to Smart Link, Monitor Link loses its significance when separately configured.

## 3.2 Configuring Basic Functions of a Smart Link Group

This section describes how to configure basic functions of a Smart Link group, such as to create a Smart Link group, enable the functions of the group, configure the master and slave interfaces, enable revertive switching, and configure Flush packets.

### [3.2.1 Establishing the Configuration Task](#)

### [3.2.2 Creating a Smart Link Group and Enabling Smart Link](#)

### [3.2.3 Configuring the Master and Slave Interfaces of the Smart Link Group](#)

### [3.2.4 \(Optional\) Enabling Revertive Switching of the Smart Link Group and Setting the WTR Time](#)

### [3.2.5 \(Optional\) Enabling the Sending of Flush Packets](#)

### [3.2.6 \(Optional\) Enabling the Receiving of Flush Packets](#)

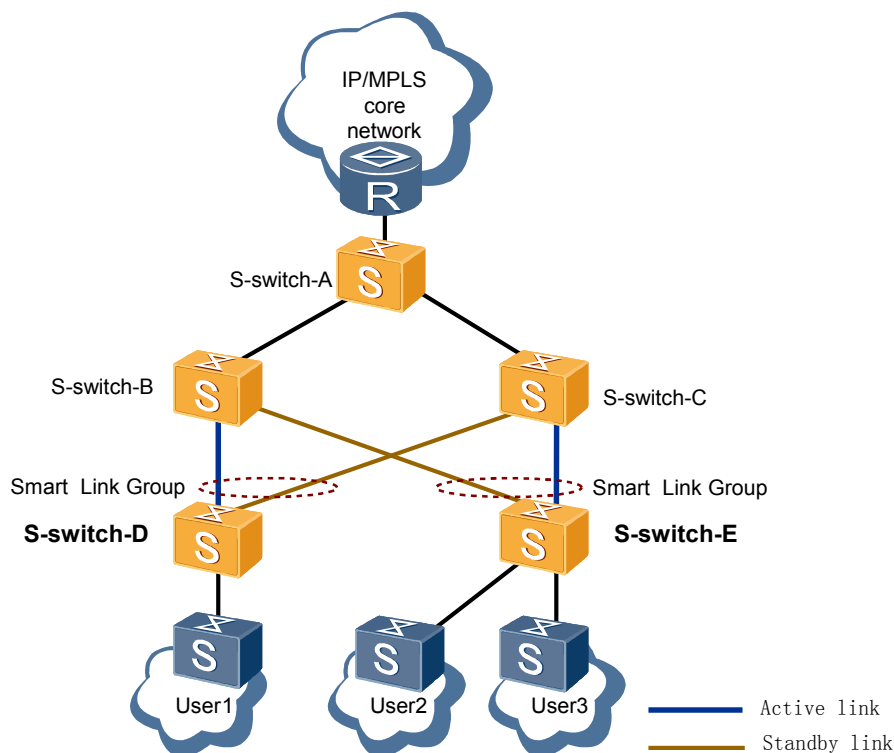
### [3.2.7 Checking the Configuration](#)

## 3.2.1 Establishing the Configuration Task

### Applicable Environment

As shown in [Figure 3-1](#), the devices at the access and convergence layer are connected to uplink devices in a dual-homed manner. This networking guarantees better security and shortens the duration of service interruption in case of link faults.

**Figure 3-1** Applicable environment of Smart Link



As shown in [Figure 3-1](#), S-switch-D and S-switch-E are connected to user devices and dual-homed to S-switch-B and S-switch-C. Configure Smart Link on S-switch-D and S-switch-E respectively and add the two uplink interfaces to the respective Smart Link group to avoid any loop. In this manner, the duration of service interruption in case of link faults can be guaranteed at the millisecond level.

### Pre-configuration Tasks

Before configuring the basic functions of a Smart Link group, complete the following tasks:

- Ensuring that the Multiple Spanning Tree Protocol (MSTP) and Rapid Ring Protection Protocol (RRPP) are not enabled on the master and slave interfaces of the Smart Link group and are not added to Eth-Trunk interfaces

### Data Preparation

To configure basic functions of the Smart Link group, you need the following data.

| No. | Data                                                   |
|-----|--------------------------------------------------------|
| 1   | Number of the interfaces added to the Smart Link group |
| 2   | ID of the Smart Link group                             |
| 3   | Control VLAN ID carried in the Flush packet            |
| 4   | Password carried in the Flush packet                   |

## 3.2.2 Creating a Smart Link Group and Enabling Smart Link

### Context

Do as follows on S-switch-D and S-switch-E shown in [Figure 3-1](#) respectively.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **smart-link group group-id** command to create a Smart Link group and enter the view of the Smart Link group. The S-switch supports a maximum of 16 Smart Link groups.
- Step 3** Run the **smart-link enable** command to enable functions of the Smart Link group.
- End

## 3.2.3 Configuring the Master and Slave Interfaces of the Smart Link Group

### Context

Do as follows on S-switch-D and S-switch-E shown in [Figure 3-1](#) respectively.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **smart-link group group-id** command to enter the view of the Smart Link group.
- Step 3** Repeatedly run the **port interface-type interface-number { master | slave }** command to add two interfaces to the Smart Link group and specify the interfaces as the master and slave interfaces.

A Smart Link group consists of a master interface and a slave interface. By default, there is no interface in a Smart Link group.

----End

## 3.2.4 (Optional) Enabling Revertive Switching of the Smart Link Group and Setting the WTR Time

### Context

Do as follows on S-switch-D and S-switch-E shown in [Figure 3-1](#) respectively.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **smart-link group group-id** command to enter the view of the Smart Link group.
- Step 3** Run the **restore enable** command to enable revertive switching of the Smart Link group.
- Be default, revertive switching of the Smart Link group is disabled.
- Step 4** (Optional) Run the **timer wtr wtr-time** command to set the wait-to-restore (WTR) time of the Smart Link group.
- By default, the WTR time of a Smart Link group is 60 seconds.
- End

## 3.2.5 (Optional) Enabling the Sending of Flush Packets

### Context

Do as follows on S-switch-D and S-switch-E shown in [Figure 3-1](#) respectively.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **smart-link group group-id** command to enter the view of the Smart Link group.
- Step 3** Run the **flush send control-vlan vlan-id [ password simple password ]** command to enable the sending of Flush packets and configure the control virtual LAN (VLAN) ID and password carried in the Flush packets.
- End

## 3.2.6 (Optional) Enabling the Receiving of Flush Packets

### Context

Do as follows on S-switch-A, S-switch-B, and S-switch-C shown in [Figure 3-1](#) respectively.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.

- Step 2** Run the **interface { ethernet | gigabitethernet } interface-number** command to enter the view of the downlink interface on S-switch-A, S-switch-B, and S-switch-C respectively.
- Step 3** Run the **smart-link flush receive control-vlan vlan-id [ password simple password ]** command to enable the receiving of Flush packets and configure the control VLAN ID and password carried in the Flush packets to be received by the interface.

**NOTE**

An interface receives Flush packets only when it is configured with the control VLAN ID and added to this VLAN. The configuration of the password is optional. If no password is specified, no password is used for authentication. Once the control VLAN ID is reconfigured, the password must be reconfigured too.

The control VLAN ID and password carried in a Flush packet received by the interface must be the same as those configured on this interface. Otherwise, the interface does not process the Flush packet.

----End

## 3.2.7 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                                      | Command                                            |
|-------------------------------------------------------------|----------------------------------------------------|
| Check information about the status of the Smart Link group. | <b>display smart-link group { all   group-id }</b> |
| Check information about the received Flush packets.         | <b>display smart-link flush</b>                    |

Run the **display smart-link group { all | group-id }** command to view information about the status of the Smart Link group. For example:

```
<Quidway> display smart-link group 1
Smart link group 1 information:
Smart link group was enable
Link status:lock
DeviceID: 00e0-fc00-0100
Member Role State Flush Count Last-Flush-Time

GigabitEthernet0/0/1 MASTER ACTVIE 1 2007/08/21 16:37:20
GGigabitEthernet0/0/2 SLAVE INACTIVE 2 2007/08/21 14:45:56
```

If the configuration is correct, the following information is displayed:

- The functions of the Smart Link group are enabled. Thus, the message "Smart link group was enabled" is displayed.
- The status of the interfaces in the Smart Link group includes the role of the interface in the group, number of sent Flush packets, and time when the Flush packets are sent. As the command output shows, GigabitEthernet 0/0/1 is the master interface in the Smart Link group; it is in the Forwarding state; it sent a Flush packet at 16:37:20 on August 21, 2007.
- Revertive switching of the Smart Link group is enabled. The WTR time is set to 30 seconds by the user.
- The control VLAN ID carried in the sent Flush packets is set by the user to 20.

Run the **display smart-link flush** command to display information about received Flush packets.

```
<Quidway> display smart-link flush
```

```
Receive flush packets count: 10
Receive last flush interface: GigabitEthernet0/0/1
Receive last flush packet time: 2007/08/21 16:19:03
Receive last flush packet source mac: 00e0-fc00-8500
Receive last flush packet control vlan ID: 1
```

## 3.3 Configuring the Data Stream Policy of the Smart Link Group

This section describes how to configure the advanced functions of the Smart Link group, such as to lock data streams and switch traffic between links manually.

### 3.3.1 Establishing the Configuration Task

### 3.3.2 Locking Data Streams to the Master Interface

### 3.3.3 Locking Data Streams to the Slave Interface

### 3.3.4 Unlocking Data Streams

### 3.3.5 Configuring the Manual Switching of Data Streams

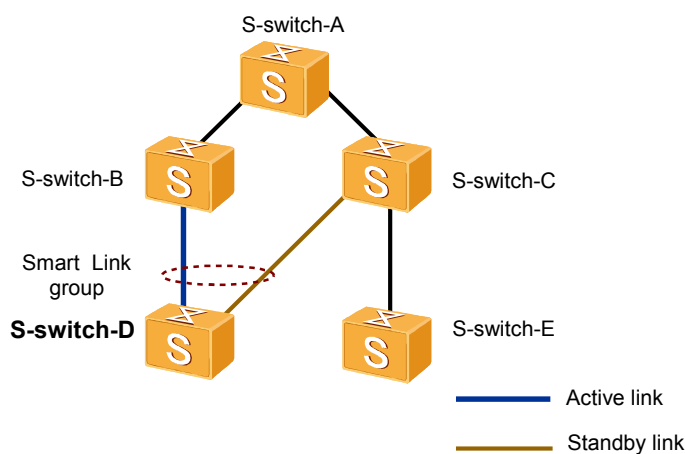
### 3.3.6 Checking the Configuration

## 3.3.1 Establishing the Configuration Task

### Applicable Environment

As shown in **Figure 3-2**, the basic functions and revertive switching of the Smart Link group are enabled on S-switch-D. During the maintenance, the active link in the Smart Link group needs to be inspected. To prevent the inspection from affecting normal services, you need to configure the data stream policy for the Smart Link group. Through the configuration, you can forcibly lock data streams to the standby link and switch them back to the active link after the inspection is complete.

**Figure 3-2** Configuring the data stream policy



## Pre-configuration Tasks

Before configuring the data stream policy of the Smart Link group, complete the following task:

- [3.2 Configuring Basic Functions of a Smart Link Group](#)

## Data Preparation

None.

### 3.3.2 Locking Data Streams to the Master Interface

#### Context

Do as follows on S-switch-D shown in [Figure 3-2](#).



#### CAUTION

If the master interface fails, the data streams locked to the master interface are not automatically switched to the slave interface. This results in service interruption.

---

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **smart-link group group-id** command to enter the view of the Smart Link group.
- Step 3** Run the **smart-link lock** command to lock data streams to the master interface.

----End

### 3.3.3 Locking Data Streams to the Slave Interface

#### Context

Do as follows on S-switch-D shown in [Figure 3-2](#).



#### CAUTION

If the slave interface fails, the data streams locked to the slave interface are not automatically switched to the master interface. This results in service interruption.

---

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **smart-link group group-id** command to enter the view of the Smart Link group.

**Step 3** Run the **smart-link force** command to lock data streams to the slave interface.

----End

### 3.3.4 Unlocking Data Streams

#### Context

Do as follows on S-switch-D shown in [Figure 3-2](#).

#### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **smart-link group group-id** command to enter the view of the Smart Link group.

**Step 3** Run the **undo smart-link lock** or **undo smart-link force** command to unlock data streams.

----End

### 3.3.5 Configuring the Manual Switching of Data Streams

#### Context

Do as follows on S-switch-D shown in [Figure 3-2](#).

#### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **smart-link group group-id** command to enter the view of the Smart Link group.

**Step 3** Run the **smart-link manual switch** command to perform the link switching.

----End

### 3.3.6 Checking the Configuration

Run the following command to check the previous configuration.

| Action                                                      | Command                                            |
|-------------------------------------------------------------|----------------------------------------------------|
| Check information about the status of the Smart Link group. | <b>display smart-link group { all   group-id }</b> |

Run the **display smart-link group { all | group-id }** command. If **Lock** is displayed, it means that data streams are locked to the master interface. If **force** is displayed, it means that data streams are locked to the slave interface.

```
<Quidway> display smart-link group 1
Smart link group 1 information:
Smart link group was enable
Link status:Lock
Wtr-time is:30
```

| DeviceID: 00e0-fc00-0100 |        | Control-vlan ID: 10 |             |                     |
|--------------------------|--------|---------------------|-------------|---------------------|
| Member                   | Role   | State               | Flush Count | Last-Flush-Time     |
| GigabitEthernet0/0/1     | MASTER | ACTVIE              | 1           | 2007/08/21 16:37:20 |
| GigabitEthernet0/0/2     | SLAVE  | INACTIVE            | 2           | 2007/08/21 14:45:20 |

## 3.4 Configuring Functions of a Monitor Link Group

This section describes how to configure functions of a Monitor Link group, such as to create a Monitor Link group, configure uplink and downlink interfaces, and enable revertive switching.

### 3.4.1 Establishing the Configuration Task

### 3.4.2 Creating a Monitor Link Group

### 3.4.3 Configuring the Uplink and Downlink Interfaces of the Monitor Link Group

### 3.4.4 Configuring the WTR Time of the Monitor Link Group

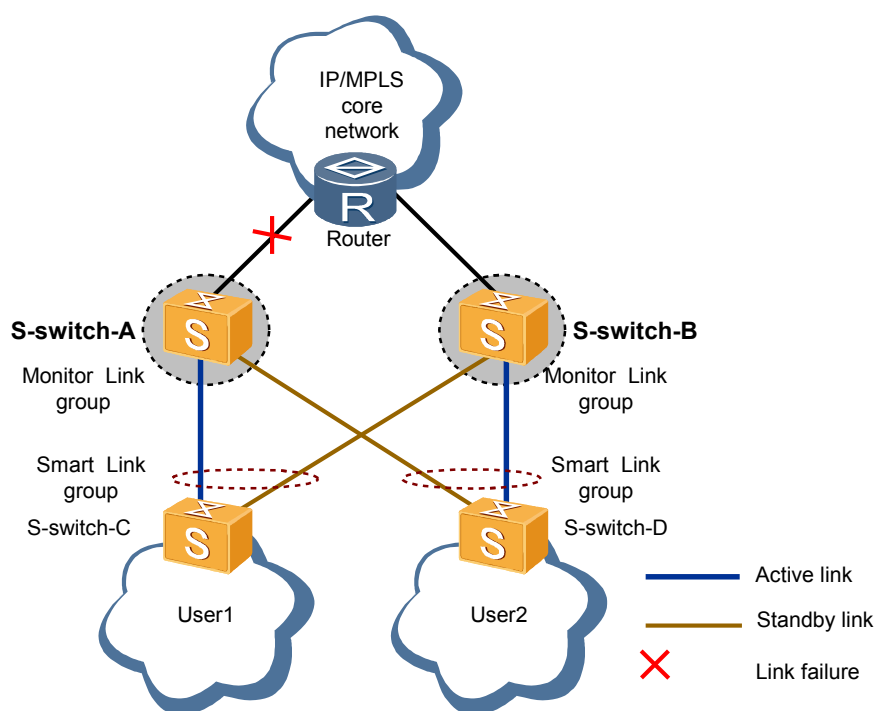
### 3.4.5 Checking the Configuration

## 3.4.1 Establishing the Configuration Task

### Applicable Environment

- As shown in [Figure 3-3](#), the S-switch with Smart Link enabled can rapidly respond when the master interface fails. The traffic is switched to the slave interface. This action shortens the duration of service interruption. If the uplink connected to the master interface, however, fails, services are interrupted too. Thus, it is required to monitor the uplink and enable the downlink to sense the fault and respond to the change.

**Figure 3-3** Applicable environment of Monitor Link



- As shown in [Figure 3-3](#), the link between S-switch-A and Router breaks. Although Smart Link is enabled on S-switch-C and S-switch-D, link switching is not performed because the active link is in good condition. In this case, services are interrupted. The device connected to the active link is configured with Monitor Link so that the Smart Link group can respond more quickly to the faults of the uplink. In this manner, the status of the uplink can be monitored. Once a fault occurs, the active link of the Smart Link group is rapidly blocked. Thus, the Smart Link group can sense the fault and start the switching between links to shorten the duration of service interruption.

## Pre-configuration Tasks

Before configuring the basic functions of the Monitor Link group, complete the following tasks:

- [3.2 Configuring Basic Functions of a Smart Link Group](#)
- Ensuring that no interface in the Monitor Link group is added to a trunk

## Data Preparation

To configure the basic functions of the Monitor Link group, you need the following data.

| No. | Data                                                    |
|-----|---------------------------------------------------------|
| 1   | ID of the Monitor Link group                            |
| 2   | Number of the interface added to the Monitor Link group |
| 3   | WTR time of the Monitor Link group                      |
| 4   | ID of the created Smart Link group                      |

## 3.4.2 Creating a Monitor Link Group

### Context

Do as follows on S-switch-A and S-switch-B shown in [Figure 3-3](#).

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **monitor-link group group-id** command to enter the view of the Monitor Link group.
- End

## 3.4.3 Configuring the Uplink and Downlink Interfaces of the Monitor Link Group

### Context

Do as follows on S-switch-A and S-switch-B shown in [Figure 3-3](#).

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **monitor-link group group-id** command to enter the view of the Monitor Link group. The S-switch supports a maximum of 16 Monitor Link groups.
- Step 3** Run the **port interface-type interface-number { downlink id | uplink }** command to specify the interface as the uplink or downlink interface of the Monitor Link group.

Or run the **smart-link group group-id uplink** command to set a Smart Link group as the uplink interface of the Monitor Link group.

### NOTE

The status of the uplink interface determines the status of the Monitor Link group. Therefore, after the downlink interface is added to the Monitor Link group, although you can run the **shutdown** or **undo shutdown** command to perform operations, operation effects last until the status of the uplink interface in the Monitor Link group is changed. After the status of the uplink interface changes, the status of the downlink interface is reconfigured.

- If the uplink interface in the Up state is added to the Monitor Link group or the uplink interface in the Down state in the Monitor Link group is changed to be in the Up state, the **undo shutdown** command is run on all downlink interfaces.
- If the uplink interface is deleted from the Monitor Link group or the uplink interface in the Up state in the Monitor Link group is changed to be in the Down state, the **shutdown** command is run on all downlink interfaces.

----End

## 3.4.4 Configuring the WTR Time of the Monitor Link Group

### Context

Do as follows on S-switch-A and S-switch-B shown in [Figure 3-3](#).

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **monitor-link group group-id** command to enter the view of the Monitor Link group.
- Step 3** Run the **timer recover-time recover-time** command to configure the WTR time for automatic revertive switching.

By default, revertive switching of a Monitor Link group is enabled and the WTR time is 3 seconds.

----End

## 3.4.5 Checking the Configuration

Run the following command to check the previous configuration.

| Action                                                   | Command                                                            |
|----------------------------------------------------------|--------------------------------------------------------------------|
| Check the basic configuration of the Monitor Link group. | <b>display monitor-link group</b> { <b>all</b>   <i>group-id</i> } |

Run the **display monitor-link group** { **all** | *group-id* } command. You can view basic information about the interfaces added to the Monitor Link group, including the role and status of the interfaces and the time when the interfaces became Up or Down for the last time.

```
<Quidway> display monitor-link group 1
Monitor link group 1 information:
Member Role State Last-up-time Last-down-time

Ethernet0/0/1 UpLk DOWN 2007/08/20 10:45:56 2007/08/21 14:45:43
Ethernet0/0/2 DwLk[1] DOWN 2007/08/21 11:45:25 2007/08/20 15:45:36
```

## 3.5 Maintaining Smart Link

This section describes how to debug Smart Link.



### CAUTION

Enabling debugging affects the system performance. Therefore, after debugging, run the **undo debugging all** command to disable debugging immediately.

If a link fails, run the following **debugging** commands in the user view to debug the link, view information about debugging, locate the fault, and then analyze the cause. For the procedure of displaying the debugging information, refer to the chapter "Monitoring and Debugging" in the *Quidway S5300 Series Ethernet Switches Configuration Guide – Device Management*.

| Action                                 | Command                                                                                                      |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Enable the debugging of Smart Link.    | <b>debugging smart-link</b> { <b>all</b>   <b>error</b>   <b>event</b> }<br>[ <b>group</b> <i>group-id</i> ] |
| Enable the debugging of Flush packets. | <b>debugging smart-link flush</b> { <b>all</b>   <b>receive</b>   <b>send</b> }                              |

## 3.6 Configuration Examples

This section provides several configuration examples of Smart Link.

### [3.6.1 Example for Configuring Basic Functions of Smart Link](#)

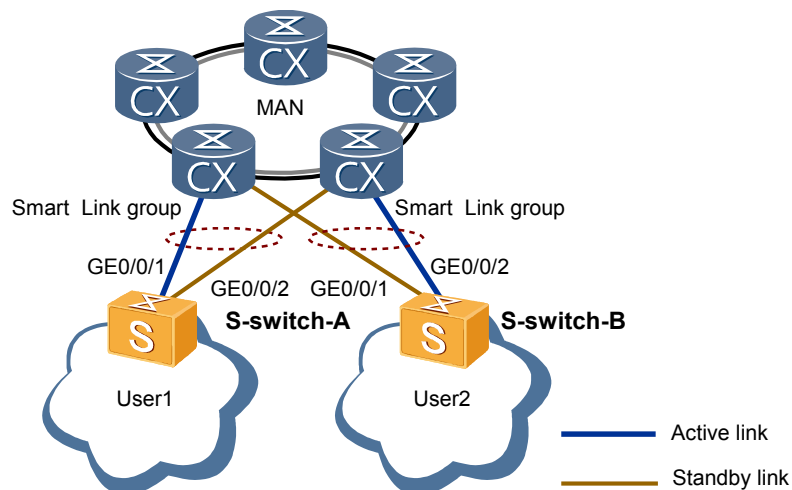
### [3.6.2 Example for Configuring the Integrated Application of Smart Link](#)

### 3.6.1 Example for Configuring Basic Functions of Smart Link

## Networking Requirements

As shown in [Figure 3-4](#), the user-side network is connected to the metropolitan area network (MAN) in a dual-homed manner to guarantee the reliability of the network. This networking ensures rapid switching of traffic to the standby link when the active link fails and service interruption lasts only several milliseconds.

**Figure 3-4** Example for configuring basic functions of Smart Link



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure Smart Link groups on S-switch-A and S-switch-B, and then add uplink interfaces to the groups.
2. Enable the revertive switching on S-switch-A and S-switch-B.
3. Enable S-switch-A and S-switch-B to send Flush packets.

## Data Preparation

To complete the configuration, you need the following data:

- Numbers of uplink interfaces configured on S-switch-A and S-switch-B
- IDs of Smart Link groups
- Control VLAN ID and password carried in Flush packets

## Configuration Procedure

1. Create the same control VLAN on S-switch-A and S-switch-B, and then add uplink interfaces to the VLAN.

The configuration details are not mentioned here. For details on the configuration, refer to the chapter "VLAN Configuration" in the *Quidway S5300 Series Ethernet Switches Configuration Guide – Ethernet*.

2. Create Smart Link groups and enable the functions of the groups.

# Configure S-switch-A.

```
<S-switch-A> system-view
```

- ```
[S-switch-A] smart-link group 1
[S-switch-A-smlk-group1] smart-link enable
```
- # Configure S-switch-B.
- ```
<S-switch-B> system-view
[S-switch-B] smart-link group 2
[S-switch-B-smlk-group2] smart-link enable
```
3. Add uplink interfaces to Smart Link groups as the master interfaces or the slave interfaces.
- # Configure S-switch-A.
- ```
[S-switch-A-smlk-group1] port gigabitethernet 0/0/1 master
[S-switch-A-smlk-group1] port gigabitethernet 0/0/2 slave
```
- # Configure S-switch-B.
- ```
[S-switch-B-smlk-group2] port gigabitethernet 0/0/2 master
[S-switch-B-smlk-group2] port gigabitethernet 0/0/1 slave
```
4. Enable the revertive switching and set the WTR time.
- # Configure S-switch-A.
- ```
[S-switch-A-smlk-group1] restore enable
[S-switch-A-smlk-group1] timer wtr 30
```
- # Configure S-switch-B.
- ```
[S-switch-B-smlk-group2] restore enable
[S-switch-B-smlk-group2] timer wtr 30
```
5. Enable the sending of Flush packets.
- # Configure S-switch-A.
- ```
[S-switch-A-smlk-group1] flush send control-vlan 10 password simple 123
```
- # Configure S-switch-B.
- ```
[S-switch-B-smlk-group2] flush send control-vlan 10 password simple 123
```
6. Verify the configuration.
- # Run the **display smart-link group** command. You can view information about the Smart Link groups on S-switch-A and S-switch-B. If the following information is displayed,
- The functions of the Smart Link group are enabled.
  - The WTR time is 30 seconds.
  - The control VLAN ID is 10.
  - GigabitEthernet 0/0/1 serves as the master interface, and GigabitEthernet 0/0/2 serves as the slave interface.
- the configuration succeeds.

```
<S-switch-A> display smart-link group 1
Smart link group 1 information:
Smart link group was enabled
Vtr-time is:30
Device ID: 00e0-fc00-0100 Control-vlan ID: 10
Member Role State Flush Count Last-Flush-Time

GigabitEthernet0/0/1 MASTER ACTIVE 0 2007/08/21 16:37:20
GigabitEthernet0/0/2 SLAVE INACTIVE 0 2007/08/21 14:45:56
```

## Configuration Files

The following lists only the configuration files of the user-side S-switches.

- Configuration file of S-switch-A
- ```
#
 sysname S-switch-A
#
```

```
vlan batch 1 10 2046
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 10
stp disable
#
smart-link group 1
smart-link enable
port GigabitEthernet0/0/1 master
port GigabitEthernet0/0/2 slave
timer wtr 30
restore enable
flush send control-vlan 10 password simple 123
#
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
vlan batch 1 10 2020
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 10
stp disable
#
smart-link group 2
smart-link enable
port GigabitEthernet0/0/2 master
port GigabitEthernet0/0/1 slave
timer wtr 30
restore enable
flush send control-vlan 10 password simple 123
#
return
```

3.6.2 Example for Configuring the Integrated Application of Smart Link

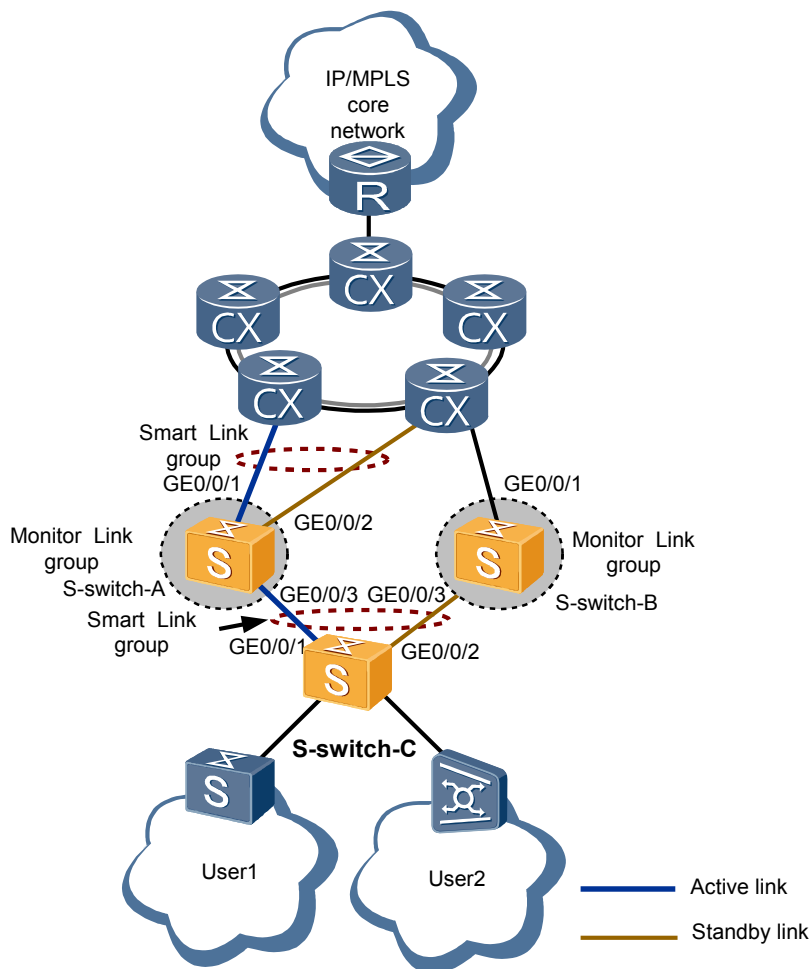
Networking Requirements

As shown in [Figure 3-5](#), connected to the downstream user network, S-switch-C on the MAN is connected to the upstream S-switch-A and S-switch-B in a dual-homed manner. S-switch-C is connected to the upstream backbone network through RRPP.

S-switch-A and S-switch-C are connected to uplink devices in a dual-homed manner. One out of each link pair needs to be blocked to avoid any loop. At the same time, when the active link fails, the data streams can be rapidly switched to the standby link to ensure normal services.

In addition, a monitoring mechanism is required to prevent the link connected to the RRPP ring from failing. Once this link fails, downstream services are interrupted. This monitoring mechanism enables the downlink to quickly sense the fault of the uplink. Once the uplink fails, link switching can be performed immediately to shorten the duration of service interruption.

Figure 3-5 Example for configuring the integrated application of Smart Link



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure Smart Link groups on S-switch-A and S-switch-C, and then add uplink interfaces to the groups.
2. Configure Monitor Link groups on S-switch-A and S-switch-B.
3. Enable S-switch-A and S-switch-C to send Flush packets.
4. Enable S-switch-A and S-switch-B to receive Flush packets.

Data Preparation

To complete the configuration, you need the following data:

- Numbers of interfaces on S-switch-A, S-switch-B, and S-switch-C
- IDs of Smart Link groups
- Control VLAN ID and password carried in Flush packets
- IDs of the Monitor Link groups and the numbers of the downlinks

Configuration Procedure

1. Configure the same control VLAN on S-switch-A, S-switch-B, and S-switch-C. Add the interfaces of the Smart Link group or Monitor Link group to this VLAN.

The configuration details are not mentioned here. For details of the configuration, refer to the chapter "VLAN Configuration" in the *Quidway S5300 Series Ethernet Switches Configuration Guide – Ethernet*.

2. Create Smart Link groups and enable the functions of the groups.

Configure S-switch-A.

```
<S-switch-A> system-view
[S-switch-A] smart-link group 1
[S-switch-A-smlk-group1] smart-link enable
```

Configure S-switch-C.

```
<S-switch-C> system-view
[S-switch-C] smart-link group 2
[S-switch-C-smlk-group2] smart-link enable
```

3. Add interfaces to Smart Link groups as the master interfaces or the slave interfaces.

Configure S-switch-A.

```
[S-switch-A-smlk-group1] port gigabitethernet 0/0/1 master
[S-switch-A-smlk-group1] port gigabitethernet 0/0/2 slave
```

Configure S-switch-C.

```
[S-switch-C-smlk-group2] port gigabitethernet 0/0/1 master
[S-switch-C-smlk-group2] port gigabitethernet 0/0/2 slave
```

4. Enable the revertive switching and set the WTR time.

Configure S-switch-A.

```
[S-switch-A-smlk-group1] restore enable
[S-switch-A-smlk-group1] timer wtr 30
```

Configure S-switch-C.

```
[S-switch-C-smlk-group2] restore enable
[S-switch-C-smlk-group2] timer wtr 30
```

5. Enable the sending and receiving of Flush packets.

Configure S-switch-A.

```
[S-switch-A-smlk-group1] flush send control-vlan 10 password simple 123
[S-switch-A-smlk-group1] quit
[S-switch-A] interface gigabitethernet 0/0/3
[S-switch-A-gigabitethernet0/0/3] smart-link flush receive control-vlan 10
password simple 123
```

Configure S-switch-B.

```
<S-switch-B> system-view
[S-switch-B] interface gigabitethernet 0/0/3
[S-switch-B-gigabitethernet0/0/3] smart-link flush receive control-vlan 10
password simple 123
```

Configure S-switch-C.

```
[S-switch-C-smlk-group2] flush send control-vlan 10 password simple 123
```

6. Create Monitor Link groups and add the uplink and downlink interfaces.

Configure S-switch-A.

```
<S-switch-A> system-view
[S-switch-A] monitor-link group 1
[S-switch-A-mtlk-group1] smart-link group 1 uplink
[S-switch-A-mtlk-group1] port gigabitethernet 0/0/3 downlink 1
```

Configure S-switch-B.

```
<S-switch-B> system-view
```

```
[S-switch-B] monitor-link group 2
[S-switch-B-mtlk-group2] port gigabitethernet 0/0/1 uplink
[S-switch-B-mtlk-group2] port gigabitethernet 0/0/3 downlink 1
```

7. Configure the WTR time of the Monitor Link groups.

Configure S-switch-A.

```
[S-switch-A-mtlk-group1] timer recover-time 10
```

Configure S-switch-B.

```
[S-switch-B-mtlk-group2] timer recover-time 10
```

Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
vlan batch 1 10 2046
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 10
stp disable
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 10
smart-link flush receive control-vlan 10 password simple 123
#
smart-link group 1
smart-link enable
port GigabitEthernet0/0/1 master
port GigabitEthernet0/0/2 slave
timer wtr 30
restore enable
flush send control-vlan 10 password simple 123
#
monitor-link group 1
smart-link group 1 uplink
port GigabitEthernet0/0/3 downlink 1
timer recover-time 10
#
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
vlan batch 1 10 2020
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 10
smart-link flush receive control-vlan 10 password simple 123
#
monitor-link group 2
port GigabitEthernet0/0/1 uplink
port GigabitEthernet0/0/3 downlink 1
timer recover-time 10
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
```

```
#
vlan batch 1 10 1032
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 10
stp disable
#
smart-link group 2
smart-link enable
port GigabitEthernet0/0/1 master
port GigabitEthernet0/0/2 slave
timer wtr 30
restore enable
flush send control-vlan 10 password simple 123
#
return
```

4 VRRP Configuration

About This Chapter

This chapter describes the principle of the Virtual Router Redundancy Protocol (VRRP), commands for maintaining VRRP, and the configurations of basic and advanced functions of VRRP as well as configuration examples.

[4.1 Introduction](#)

This section describes the basic concepts of VRRP and VRRP features supported by the S-switch.

[4.2 Configuring a VRRP Backup Group](#)

This section describes how to create a VRRP backup group, assign the virtual IP address, and set the priority of each interface in the VRRP backup group.

[4.3 Configuring VRRP to Track the Status of an Interface](#)

This section describes how to configure VRRP to track the interface status to improve system reliability.

[4.4 Configuring VRRP Fast Switchover](#)

This section describes how to configure VRRP to track a BFD session to implement fast switchover.

[4.5 Configuring VRRP on VLANIF Interfaces](#)

This section describes how to configure VRRP on VLANIF interfaces.

[4.6 Configuring the VRRP Security Function](#)

This section describes how to implement VRRP authentication.

[4.7 Adjusting and Optimizing VRRP](#)

This section describes how to adjust the related parameters of VRRP packets to optimize VRRP.

[4.8 Maintaining VRRP](#)

This section describes how to debug VRRP.

[4.9 Configuration Examples](#)

This section describes how to configure a VRRP backup group.

4.1 Introduction

This section describes the basic concepts of VRRP and VRRP features supported by the S-switch.

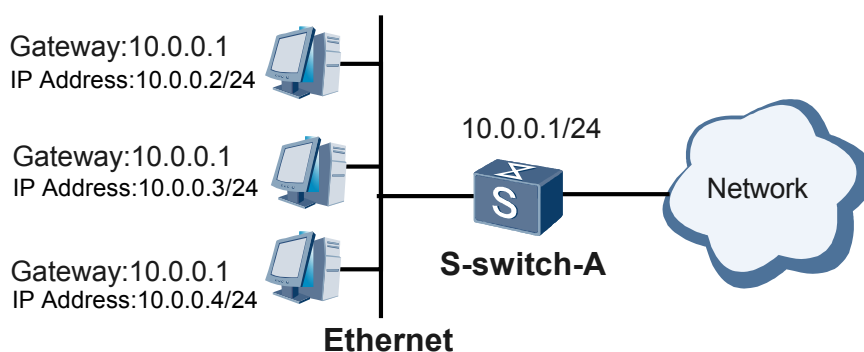
4.1.1 VRRP Overview

4.1.2 VRRP Features Supported by the S-switch

4.1.1 VRRP Overview

In general, all hosts in an internal network are configured with the same default route. Internal hosts send the packets whose destination addresses are not on the local network segment to the default egress gateway, such as the S-switch in [Figure 4-1](#). Thus, the internal hosts and external network can communicate with each other. When the egress gateway is Down, however, all the hosts using this gateway fail to communicate with external network.

Figure 4-1 Default gateway in a LAN



The common method to improve system reliability is to deploy multiple egress gateways. In addition, the problem of selecting routes among these gateways should be solved.

VRRP is a fault-tolerant protocol defined in RFC 3768. VRRP solves the problem of route selection among egress gateways by separating physical devices from logical devices.

In a Virtual Local Area Network (LAN) with multicast and broadcast capabilities (like the Ethernet), VRRP uses logical gateways to ensure high availability of transmission links. This prevents service interruption that results from a gateway device failure, without changing the configuration of routing protocols.

4.1.2 VRRP Features Supported by the S-switch

Master/Backup Mode

The master/backup mode is the basic mode provided by VRRP for backing up the IP address of a VRRP backup group. In master/backup mode, a VRRP backup group consists of a master S-switch and multiple backup S-switches. Different S-switches have different priorities in the backup group. The S-switch with the highest priority serves as the master S-switch.

- The master S-switch undertakes all services in normal condition.
- A backup S-switch may undertake services only when the master S-switch fails.

Load Balancing Mode

For the load balancing mode, two or more backup groups are created. Multiple backup groups undertake services at the same time.

In load balancing mode, the VRRP backup groups have the following features:

- A S-switch can join several VRRP backup groups and has different priorities in different backup groups. Multiple virtual S-switches are configured to carry out load balancing.
- Each backup group consists of a master S-switch and multiple backup S-switches.
- The master S-switches of the backup groups can be different.

Tracking the Interface Status

The S-switch can track interface status.. When the status of an interface changes, the priority of the S-switch in the backup group is automatically adjusted. The order of the priorities of the S-switches in the backup group change and a new master S-switch is selected.

Enabling and disabling the Ping to the Virtual IP Address

Because VRRP backup groups use virtual IP addresses, it brings troubles if the virtual IP address of a VRRP backup group cannot be pinged through. You may ping through the virtual IP address to monitor the operating status of the virtual S-switches, but the VRRP backup group may suffer the Internet Control Message Protocol (ICMP) attack. On the S-switch, you can enable and disable the ping to the virtual IP address as required.

VRRP Security Function

For networks of different security levels, you can set different authentication modes and authentication keys in the headers of VRRP packets.

In a secure network, you can adopt the default configuration. That is, the S-switch does not authenticate the VRRP packets to be sent and received. The S-switch considers all the received packets as valid VRRP packets. In this case, no authentication key is required.

In an insecure network, VRRP provides simple text authentication. You can set an authentication key ranging from 1 to 8 characters.

4.2 Configuring a VRRP Backup Group

This section describes how to create a VRRP backup group, assign the virtual IP address, and set the priority of each interface in the VRRP backup group.

[4.2.1 Establishing the Configuration Task](#)

[4.2.2 Creating a Backup Group and Configuring the Virtual IP Address](#)

[4.2.3 Configuring the Priority of an Interface in a Backup Group](#)

[4.2.4 Checking the Configuration](#)

4.2.1 Establishing the Configuration Task

Applicable Environment

A VRRP backup group can work in either master/backup mode or load balancing mode.

- Master/backup switchover is a basic function provided by VRRP. The master/backup mode functions as follows:
 - Only one backup group exist.
 - The S-switch with the highest priority in the backup group serves as the master S-switch and undertakes communications services.
 - Other S-switchs in the backup group serve as the backup S-switchs and work in the backup state.
 - If the master S-switch fails, the backup S-switchs select a new master S-switch based on their priorities to provide routing services.
- In load balancing mode, multiple backup groups are created to share the traffic of a network. A S-switch can join different backup groups. The load balancing mode functions as follows:
 - S-switchA serves as the master device in backup group 1 and the backup device in backup group 2.
 - S-switchB serves as the master device in backup group 2 and the backup device in backup group 1.
 - Some hosts on the network use backup group 1 as their gateways and others use backup group 2 as their gateways.

In this case, S-switchA and S-switchB can back up each other and share traffic.

Pre-configuration Tasks

Before configuring a VRRP backup group, complete the following tasks:

- Configuring physical parameters for the interfaces in the VRRP backup group
- Configuring link layer attributes for the interfaces in the VRRP backup group
- Configuring network layer attributes for the interfaces in the VRRP backup group to ensure network connectivity

Data Preparation

To configure a VRRP backup group, you need the following data.

No.	Data
1	Backup group ID
2	Virtual IP address of the backup group
3	Priorities of the S-switchs in the VRRP backup group

4.2.2 Creating a Backup Group and Configuring the Virtual IP Address

Context

Do as follows on each S-switch in the backup group.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface interface-type interface-number** command to enter the interface view.

Step 3 Run the **vrrp vrid virtual-router-id virtual-ip virtual-address** command to create a backup group and configure the virtual IP address.

NOTE

- The virtual IP addresses of different backup groups must be different.
- In the same VLAN, the *virtual-router-ids* must be different.
- Both ends of the same backup group must be configured with the same *virtual-router-id*.

When you assign the first IP address to a VRRP backup group, the system creates this backup group.

Then, when you assign another virtual IP address to the backup group, the system adds this address into the virtual IP address list of this backup group.

For users who require equivalent VRRP reliability, a backup group can be configured with multiple virtual IP addresses. Different addresses serve different user groups. This is easy to manage and prevents users' default gateway addresses from varying with the VRRP configuration. A maximum of 16 virtual IP addresses can be assigned to a backup group.

For VRRP backup groups working in load balancing mode, you need to repeat the procedure to configure multiple backup groups on an interface. At least two backup groups are required on an interface. Backup groups are identified by *virtual-router-ids* and their virtual IP addresses must be different.

NOTE

The maximum of 255 backup groups can be configured on an interface.

NOTE

To configure VRRP and static ARP simultaneously on a device, note that when VRRP is configured on a VLANIF interface, you cannot use the IP addresses on the static ARP entries related to this interface as VRRP virtual IP addresses. Otherwise, incorrect host routes are generated and abnormal forwarding between the devices may take place.

----End

4.2.3 Configuring the Priority of an Interface in a Backup Group

Context

The master/backup mode requires only one backup group. Devices have different priorities in this backup group. The S-switch with the highest priority serves as the master S-switch and other S-switches are in the backup state.

The load balancing mode requires two or more backup groups. Each S-switch has different priorities in different backup groups. VRRP identifies the role of a S-switch in a backup group according to the priority. You can repeat configuring the priority of a S-switch to ensure that the masters of the VRRP backup groups are distributed on different S-switches.

Do as follows on the interface of each S-switch in the backup groups.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **vrrp vrid virtual-router-id priority priority-value** command to set the priority of the S-switch in the backup group.

By default, the priority is 100.

The priority of 0 is reserved for the special purpose. The priority of 255 is reserved for the IP address owner and this priority cannot be changed. You can set the priority to a value ranging from 1 to 254 through commands.

----End

4.2.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the status of VRRP.	display vrrp [interface vlanif vlan-id [virtual-router-ID]]

For the master/backup mode, after the configuration, you can run the **display vrrp** command to view the status of the VRRP backup group.

```
<Quidway> display vrrp
Vlanif10 | Virtual Router 1
state : Master
Virtual IP : 10.1.1.111
PriorityRun : 120
PriorityConfig : 120
MasterPriority : 120
Preempt : YES Delay Time : 20
Timer : 1
Auth Type : NONE
Check TTL : YES
```

For the load balancing mode, after the configuration, you can run the **display vrrp** command to view the status of a S-switch in different backup groups.

```
<Quidway> display vrrp
```

```
Vlanif10 | Virtual Router 1
  state : Master
  Virtual IP : 10.1.1.111
  PriorityRun : 120
  PriorityConfig : 120
  MasterPriority : 120
  Preempt : YES    Delay Time : 0
  Timer : 1
  Auth Type : NONE
  Check TTL : YES
Vlanif20 | Virtual Router 2
  state : Backup
  Virtual IP : 10.1.1.112
  PriorityRun : 100
  PriorityConfig : 100
  MasterPriority : 120
  Preempt : YES    Delay Time : 0
  Timer : 1
  Auth Type : NONE
  Check TTL : YES
```

4.3 Configuring VRRP to Track the Status of an Interface

This section describes how to configure VRRP to track the interface status to improve system reliability.

[4.3.1 Establishing the Configuration Task](#)

[4.3.2 Configuring VRRP to Track the Status of an Interface](#)

[4.3.3 Checking the Configuration](#)

4.3.1 Establishing the Configuration Task

Applicable Environment

VRRP can track the status of interfaces. That is, VRRP provides backup routes when a fault occurs to an interface in the backup group or other interfaces on the S-switch.

The methods of tracking the interface status are as follows:

- When the tracked interface is Down, the priority of the S-switch in the backup group reduces by a certain value automatically to be lower than those of other S-switches in the group.
- The S-switch with the highest priority becomes the master S-switch and completes the switchover.

Pre-configuration Tasks

Before configuring VRRP to track the status of an interface, complete the following tasks:

- Configuring physical parameters for the interface in the VRRP backup group
- Configuring link layer attributes for the interface in the VRRP backup group
- Configuring network layer attributes for the interface in the VRRP backup group to ensure network connectivity
- Configuring the VRRP backup group

Data Preparation

To configure VRRP to track the status of an interface, you need the following data.

No.	Data
1	Backup group ID
2	Interface to be tracked and the value by which the priority increases or decreases

4.3.2 Configuring VRRP to Track the Status of an Interface

Context

Backup can be performed when other interfaces on the S-switch are unavailable. This feature is required in Network Address Translation (NAT) applications.

Do as follows on the S-switch where the interface to be tracked locates.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **vrrp vrid virtual-router-id track interface interface-type interface-number [increased value-increased | reduced value-reduced]** command to track the specified interface.

By default, when the tracked interface is Down, its priority decreases by 10.

increased value-increased: specifies the value by which the priority increases when the tracked interface goes Up. The value ranges from 1 to 255. The highest priority is 254.

reduced value-reduced: specifies the value by which the priority decreases when the tracked interface goes Down. The value ranges from 1 to 255. The lowest priority is 1.

----End

4.3.3 Checking the Configuration

Run the following command to check the configuration.

Action	Command
Check the status of VRRP.	display vrrp [interface vlanif vlan-id [virtual-router-ID]]

```
<Quidway> display vrrp
Vlanif10 | Virtual Router 1
State : Master
Virtual IP : 10.1.1.111
PriorityRun : 130
```

```
PriorityConfig : 130
MasterPriority : 130
Preempt : YES   Delay Time : 0
Timer : 1
Auth Type : NONE
Check TTL : YES
Track if : Vlanif20   priority reduced : 10
IF State : UP
```

You can run the **display vrrp** command to view the **track if** and **IF State** fields. In the **track if** field, the type and number of the tracked interface are displayed. In the **IF State** field, the Up or Down state of the tracked interface is displayed.

4.4 Configuring VRRP Fast Switchover

This section describes how to configure VRRP to track a BFD session to implement fast switchover.

4.4.1 Establishing the Configuration Task

4.4.2 Tracking the BFD Session Status

4.4.3 Checking the Configuration

4.4.1 Establishing the Configuration Task

Applicable Environment

You can apply VRRP to track a BFD session. After being notified of the BFD session change, the VRRP module increases or decreases the priority according to the configuration to perform fast VRRP switchover.

When the VRRP backup group tracks a common BFD session and the status of the BFD session changes, the master/backup switchover is performed through the change of the priority of the S-switch. When the tracked common BFD session is restored, the priority of the S-switch in the VRRP backup group is also restored to the original value..

Pre-configuration Tasks

Before configuring VRRP fast switchover, complete the following tasks:

- Configuring physical parameters for the interfaces in the VRRP backup group
- Configuring link layer attributes for the interfaces in the VRRP backup group
- Configuring network layer attributes for the interfaces in the VRRP backup group to ensure network connectivity
- Configuring the VRRP backup group
- Configuring the BFD session

Data Preparation

To configure VRRP fast switchover, you need the following data.

No.	Data
1	Backup group ID
2	ID of the BFD sessions that is tracked and the value by which the priority increases or decreases

4.4.2 Tracking the BFD Session Status

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface vlanif *vlan-id*** command to enter the VLANIF interface view.
- Step 3** Run the **vrrp vrid *virtual-router-id* track bfd-session *bfd-session-id* [**increased** *value-increased* | **reduced** *value-reduced*]** command to track the common BFD session.

increased *value-increased*: specifies the value by which the priority increases when the tracked BFD session goes Up. The value ranges from 1 to 255. The highest priority is 254.

reduced *value-reduced*: specifies the value by which the priority decreases when the tracked BFD session goes Down. The value ranges from 1 to 255. The lowest priority is 1. By default, when the tracked BFD session goes Down, its priority decreases by 10.

When setting the value by which the priority increases or decreases, note that the increased or decreased value must be higher or lower than the priority of another S-switch in the backup group to implement fast VRRP switchover. Pay attention to this point especially when using the default value.

----End

4.4.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the VRRP status.	display vrrp [interface <i>interface-type</i> <i>interface-number</i> [<i>virtual-router-id</i>]]

Run the **display vrrp** command, and you can view that the BFD session that is tracked by VRRP is Up. The command output is as follows:

```
<Quidway> display vrrp
Vlanif10 | Virtual Router 1
state : Backup
Virtual IP : 192.168.1.100
```

```
PriorityRun : 120
PriorityConfig : 120
MasterPriority : 130
Preempt : YES    Delay Time : 0
Timer : 1
Auth Type : NONE
Check TTL : YES
Track BFD : 1    Priority increased : 20
BFD-Session State : Up
```

4.5 Configuring VRRP on VLANIF Interfaces

This section describes how to configure VRRP on VLANIF interfaces.

[4.5.1 Establishing the Configuration Task](#)

[4.5.2 Configuring VRRP on VLANIF Interfaces](#)

[4.5.3 \(Optional\) Setting the Sending Mode of VRRP Packets in the Super-VLAN](#)

[4.5.4 Checking the Configuration](#)

4.5.1 Establishing the Configuration Task

Applicable Environment

VLANIF interfaces support VRRP.

Pre-configuration Tasks

Before configuring VRRP on VLANIF interfaces, complete the followings tasks:

- Configuring physical parameters for the interfaces in the VRRP backup group
- Configuring link layer attributes for the interfaces in the VRRP backup group
- Creating a sub-VLAN
- Creating a super-VLAN

Data Preparation

To configure VRRP on VLANIF interfaces, you need the following data.

No.	Data
1	Super-VLAN ID
2	Sub-VLAN ID
3	Backup group ID
4	Virtual IP address of the backup group

4.5.2 Configuring VRRP on VLANIF Interfaces

Context

Do as follows on the S-switchs where the VLANIF interfaces locate.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface vlanif *vlan-id*** command to enter the VLANIF interface view.
- Step 3** Run the **vrrp vrid *virtual-router-id* virtual-ip *virtual-address*** command to create a backup group and assign a virtual IP address to the backup group.
- Step 4** Run the **vrrp vrid *virtual-router-id* priority *priority-value*** command to set the priority of the S-switch in the backup group.

----End

4.5.3 (Optional) Setting the Sending Mode of VRRP Packets in the Super-VLAN

Context

Do as follows on the S-switchs that are configured with VRRP and the super-VLAN.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface vlanif *vlan-id*** command to enter the VLANIF interface view.
- Step 3** Run the **vrrp advertise send-mode { *sub-vlan-id* | all }** command to set the sending mode of VRRP packets.

By default, a super-VLAN does not send VRRP packets to its sub-VLANs.

----End

4.5.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the status of VRRP.	display vrrp [interface <i>interface-type</i> <i>interface-number</i> [<i>virtual-router-id</i>]]

After the configuration, run the **display vrrp interface vlanif** command, and you can view the VRRP status on the VLANIF interfaces.

```
<Quidway> display vrrp interface vlanif 40
Vlanif40 | Virtual Router 1
State : Master
Virtual IP : 100.1.1.111
```

```
PriorityRun : 120
PriorityConfig : 120
MasterPriority : 120
Preempt : YES    Delay Time : 0
Timer : 1
Auth Type : NONE
Check TTL : YES
```

4.6 Configuring the VRRP Security Function

This section describes how to implement VRRP authentication.

4.6.1 Establishing the Configuration Task

4.6.2 Setting the Authentication Mode for VRRP Packets

4.6.3 Checking the Configuration

4.6.1 Establishing the Configuration Task

Applicable Environment

In a secure network, by default, the S-switch considers VRRP packets valid without authenticating them. In this case, you need not configure an authentication key.

In an insecure network, VRRP supports simple text authentication. You can set an authentication key ranging from 1 to 8 characters.

The process of simple text authentication is as follows:

- The transmitter adds the authentication key to VRRP packets.
- The receiver compares the received authentication key with the local authentication key. If they are the same, VRRP packets are valid. Otherwise, the receiver discards the received VRRP packets and sends a trap to the Network Management System (NMS).

Pre-configuration Tasks

Before configuring the VRRP security function, complete the following tasks:

- Configuring physical parameters for the interfaces in the VRRP backup group
- Configuring link layer attributes for the interfaces in the VRRP backup group
- Configuring network layer attributes for the interfaces in the VRRP backup group to ensure network connectivity
- Configuring the VRRP backup group

Data Preparation

To configure the VRRP security function, you need the following data.

No.	Data
1	Backup group ID
2	Virtual IP address of the backup group

No.	Data
3	Authentication key of VRRP packets

4.6.2 Setting the Authentication Mode for VRRP Packets

Context

Do as follows on the S-switchs where the authentication mode for VRRP packets need to be set.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface vlanif *vlan-id*** command to enter the VLANIF interface.

Step 3 Run the **vrrp authentication-mode simple *key*** command to set the authentication mode for VRRP packets.

Set the same authentication key on the master S-switch and the backup S-switchs.

----End

4.6.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the status of VRRP.	display vrrp [interface vlanif <i>vlan-id</i> [virtual-router-<i>ID</i>]]

After the configuration, run the **display vrrp** command, and you can view the authentication mode of VRRP packets.

```
<Quidway> display vrrp
vlanif10 | Virtual Router 1
  State : Master
  Virtual IP : 10.1.1.111
  PriorityRun : 120
  PriorityConfig : 120
  MasterPriority : 120
  Preempt : YES    Delay Time : 20
  Timer : 1
  Auth Type : SIMPLE TEXT    Auth key : hello
  Check TTL : YES
```

According to the preceding command output, the **Auth Type** field displays **SIMPLE TEXT** and the **Auth key** field displays **hello**. That is, the authentication mode of VRRP packets is simple text authentication and the authentication key is **hello**.

4.7 Adjusting and Optimizing VRRP

This section describes how to adjust the related parameters of VRRP packets to optimize VRRP.

[4.7.1 Establishing the Configuration Task](#)

[4.7.2 Configuring the Interval for Sending VRRP Advertisement Packets](#)

[4.7.3 Configuring the Preemption Delay for the S-switchs in the Backup Group](#)

[4.7.4 Ping to the Virtual IP Address](#)

[4.7.5 Disabling the Detection of the TTL Value of VRRP Packets](#)

[4.7.6 Configuring the Timeout Period for the Master S-switch to Send Gratuitous ARP Packets](#)

[4.7.7 Configuring the VRRP NMS](#)

[4.7.8 Checking the Configuration](#)

4.7.1 Establishing the Configuration Task

Applicable Environment

You can configure the related parameters of VRRP packets to optimize the functions of a backup group.

- By increasing the interval for sending VRRP advertisement packets in the backup group, you can reduce the network load caused by the transmission of negotiation packets; By setting the same interval for sending VRRP advertisement packets on the members of the backup group, you can avoid coexistence of multiple masters in the backup group.
- By configuring the preemption mode and preemption delay time on the S-switchs in the backup group, you can increase or reduce the speed of the master/backup switchover.
- By enabling the test on the reachability of the virtual IP address, you can ping the virtual IP address to check the network connectivity.
- By barring the test on TTL of VRRP packets, you can improve the compatibility of Huawei devices and non-Huawei devices.
- By configuring the NMS, you can send traps to notify the NMS of communication failures.

Pre-configuration Tasks

Before adjusting and optimizing VRRP, complete the following tasks:

- Configuring physical parameters for the interfaces in the VRRP backup group
- Configuring link layer attributes for the interfaces in the VRRP backup group
- Configuring network layer attributes for the interfaces in the VRRP backup group to ensure network connectivity
- Configuring the VRRP backup group

Data Preparation

To adjust and optimize VRRP, you need the following data.

No.	Data
1	Interval for sending VRRP advertisement packets
2	Preemption delay of the S-switchs in the backup group
3	Timeout period for the master to send gratuitous ARP packets

4.7.2 Configuring the Interval for Sending VRRP Advertisement Packets

Context

The master S-switch sends VRRP advertisement packets at intervals to notify the backup S-switchs that it functions normally. If the backup S-switchs do not receive VRRP advertising messages when the timer times out, the backup S-switch with the highest priority becomes the master S-switch automatically.

Do as follows on the master S-switch to adjust the interval for sending VRRP advertisement packets.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **vrrp vrid virtual-router-id timer advertise advertise-interval** command to set the interval for sending VRRP advertisement packets.

By default, the interval for sending VRRP advertisement packets is 1 second. When multiple backup groups exist, sending VRRP advertisement packets at very short intervals may lead to frequent VRRP switchover. In this case, you can increase the interval.

----End

4.7.3 Configuring the Preemption Delay for the S-switchs in the Backup Group

Context

Do as follows on the S-switchs in the VRRP backup group where the preemption delay needs to be adjusted.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.

Step 3 Run the **vrrp vrid** *virtual-router-id* **preempt-mode timer delay** *delay-value* command to set the preemption delay.

By default, the preemption mode is adopted and the preemption delay is 0s, that is, immediate preemption.

In immediate preemption mode, a backup S-switch becomes the new master S-switch when its priority is higher than that of the current master S-switch. The original master S-switch becomes a backup S-switch. After the preemption delay is set, the backup S-switch preempt to be the master S-switch after the delay.

----End

Postrequisite

Run the **vrrp vrid** *virtual-router-id* **preempt-mode disable** command to configure the non-preemption mode on the S-switchs in the backup group. In non-preemption mode, if a S-switch in the backup group becomes the master S-switch and works normally, other S-switchs do not become the master S-switch even if they are configured with higher priorities later.

Run the **undo vrrp vrid** *virtual-router-id* **preempt-mode** command to restore the default preemption mode.

After the IP address owner recovers from a fault, it switches to be the master S-switch immediately without waiting the preemption delay. The preemption delay refers to a delay period for the backup S-switch to switch to be the master S-switch. The preemption delay is unavailable to the IP address owner. For the VRRP backup group that needs to support the preemption delay, the master virtual S-switch cannot be configured as the IP address owner.

NOTE

On each S-switch to be configured with a delay mode in a VRRP backup group, it is recommended to configure the backup S-switchs with the immediate preemption mode (whose delay time is 0s) and configure the master S-switch with the preemption mode (whose delay time is specified). Configuring the delay time for the master S-switch can ensure that the original primary link has enough time to restore and work stably, and then switch back. At the same time, the secondary link works normally. If the data is switched back to the original primary link, the application is not affected.

4.7.4 Ping to the Virtual IP Address

Context

On the S-switch, you can ping the virtual IP address to check the following items:

- Whether the master S-switch in the backup group is available.
- Whether the internal user can access external networks through the virtual IP address that serves as the default gateway.

Do as follows on the S-switchs where the virtual IP address need to be pinged.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **vrrp virtual-ip ping enable** command to ping the virtual IP address.

By default, the ping function is enabled. The master S-switch responds to the ping packets of the virtual IP address of this backup group.

----End

Postrequisite

If you ping through the virtual IP address, the ICMP attack may occur.

Running the **undo vrrp virtual-ip ping enable** command, you can cancel the ping to the virtual IP address.

4.7.5 Disabling the Detection of the TTL Value of VRRP Packets

Context

As defined in RFC 3768, the system detects the TTL value in the received VRRP packets. The packets whose TTL value is not 255 are discarded.

In certain networking environments where Huawei devices and non-Huawei devices work together, detecting the TTL value of VRRP packets may result in discarding VRRP packets incorrectly. You can configure the system not to detect the TTL value of VRRP packets.

Do as follows on the S-switches to be disabled from detecting the TTL value of VRRP packets.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
 - Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
 - Step 3** Run the **vrrp un-check ttl** command to disable the detection of the TTL value of VRRP packets.
By default, the TTL value of VRRP packets is detected.
You can run the **undo vrrp un-check ttl** command to detect the TTL value of VRRP packets.
- End

4.7.6 Configuring the Timeout Period for the Master S-switch to Send Gratuitous ARP Packets

Context

Do as follows on the master S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vrrp gratuitous-arp timeout** *time* command to configure the timeout period for the master S-switch to send gratuitous ARP packets.
The master S-switch sends ARP packets with the virtual MAC address.

By default, the master S-switch sends a gratuitous ARP packet every 300 seconds (5 minutes).

----End

Postrequisite

Run the **undo vrrp gratuitous-arp timeout** command in the system view to restore the default timeout period for the master S-switch to send gratuitous ARP packets.

Run the **vrrp gratuitous-arp timeout disable** command in the system view to disable the master S-switch from sending gratuitous ARP packets.

4.7.7 Configuring the VRRP NMS

Context

Do as follows on the S-switches to be enabled with the VRRP NMS.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **snmp-agent trap enable vrrp** command to enable the VRRP module to send traps to the NMS.

By default, the VRRP module can send traps.

NOTE

You need to enable SNMP globally before running this command.

----End

4.7.8 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the status of VRRP.	display vrrp [interface vlanif <i>vlan-id</i> [<i>virtual-router-ID</i>]]

```
<Quidway> display vrrp
Vlanif40 | Virtual Router 1
  State : Master
  Virtual IP : 100.1.1.111
  PriorityRun : 120
  PriorityConfig : 120
  MasterPriority : 120
  Preempt : YES    Delay Time : 0
  Timer : 20
  Auth Type : NONE
  Check TTL : YES
```

Run the **display vrrp** command, and you can view the modified VRRP parameter. For example, the **Timer** field displays **20**. That is, the interval for sending the VRRP advertisement packet is modified to 20 seconds. The default interval is 1 second.

4.8 Maintaining VRRP

This section describes how to debug VRRP.

4.8.1 Monitoring the VRRP Running Status

4.8.2 Debugging VRRP

4.8.1 Monitoring the VRRP Running Status

In routine maintenance, you can run the following command in any view to display the running status of VRRP.

Action	Command
Check the current running status and parameters of VRRP.	display vrrp [interface <i>interface-type</i> <i>interface-number</i> [<i>virtual-router-ID</i>]]

4.8.2 Debugging VRRP

When a VRRP fault occurs, run the following **debugging** commands in the user view to debug VRRP and locate the fault.



CAUTION

Debugging affects the performance of the system. After debugging, run the **undo debugging all** command to disable it immediately.

Action	Command
Enable the debugging of VRRP packets.	debugging vrrp packet [vrid <i>virtual-router-id</i>]
Enable the debugging of VRRP status.	debugging vrrp state [vrid <i>virtual-router-id</i>]
Enable the debugging of VRRP timer.	debugging vrrp timer [vrid <i>virtual-router-id</i>]

4.9 Configuration Examples

This section describes how to configure a VRRP backup group.

4.9.1 Example for Combining NAT and VRRP

4.9.2 Example for Configuring VRRP in Master/Backup Mode

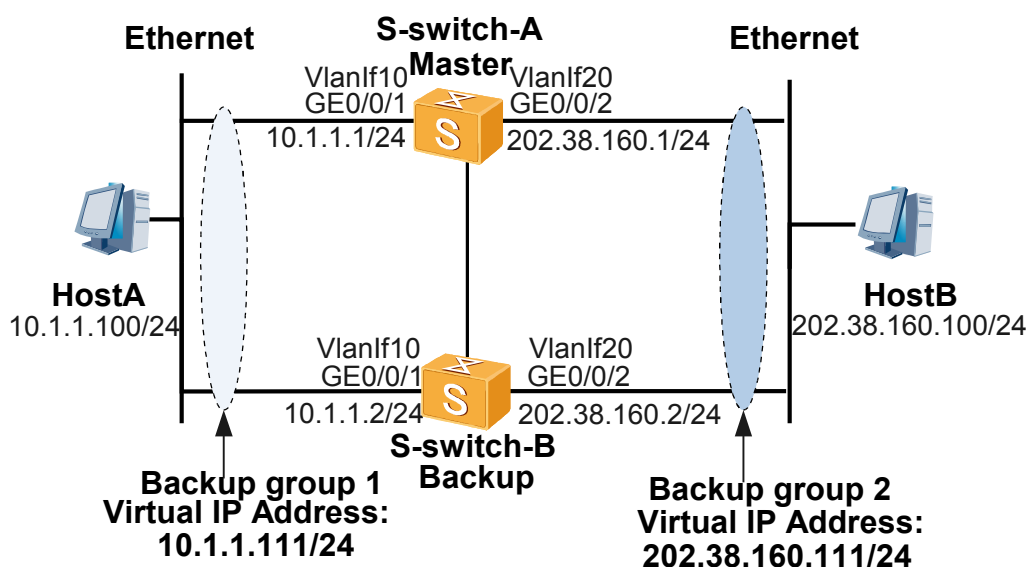
4.9.3 Example for Configuring VRRP in Load Balancing Mode

4.9.1 Example for Combining NAT and VRRP

Networking Requirements

As shown in **Figure 4-2**, S-switch-A and S-switch-B respectively connect the internal and external networks. Enable NAT on the interfaces connecting to the external network to hide information about the internal network.

Figure 4-2 Networking diagram of combining NAT and VRRP



For NAT, a transfer table is created on S-switch-A and S-switch-B respectively. When the information flow matches the transfer entry, the information flow can return normally.

After multiple backup groups are configured and specified interfaces are tracked, the status of VRRP backup groups can be kept consistent and NAT traversal can perform normally.

Configuration Roadmap

The configuration roadmap is as follows:

1. S-switch-A serves as the master and S-switch-B serves as the backup S-switch. Normally, S-switch-A is assumed as a gateway.
2. Configure VRRP backup groups on the interfaces connecting to the internal and external networks respectively on S-switch-A and S-switch-B. The backup groups on a S-switch tracks the interfaces of each other. Thus, the status of VRRP backup groups on the same S-switch are the same. That is, the S-switch serves as the master router or backup router in both backup groups.

Data Preparation

To complete the configuration, you need the following data:

- Virtual IP addresses and IDs of the VRRP backup groups
- Priorities of the S-switchs in backup groups

Configuration Procedure

1. Configure interconnection between the S-switchs. The detailed configuration is not mentioned here.

Set the virtual IP address the default gateway of Host A to 10.1.1.111 in backup group 1 and the IP address of the default gateway of Host B to 202.38.160.111 in backup group 2.

Enable OSPF between S-switchA and S-switch-B.

2. Configure VRRP.

Create backup group 1 on Vlanif 10 that connects the internal network on S-switch-A. The priority of S-switch-A in backup group 1 is 120. S-switch-A serves as the master S-switch and tracks Vlanif 20 that connects the external network.

```
<RouterA> system-view
[RouterA] vlan 10
[S-switch-A-vlan10] port GigabitEthernet 0/0/1
[S-switch-A-vlan10] interface vlanif10
[S-switch-A-vlanif10] ip address 10.1.1.1 24
[S-switch-A-vlanif10] vrrp vrid 1 virtual-ip 10.1.1.111
[S-switch-A-vlanif10] vrrp vrid 1 priority 120
[S-switch-A-vlanif10] vrrp vrid 1 track interface GigabitEthernet 0/0/2
reduced 30
[S-switch-A-vlanif10] quit
```

Create backup group 2 on Vlanif 20 connecting the external network on S-switch-A. The priority of S-switch-A in backup group 2 is 120 (as the master router). Backup group 2 tracks Vlanif 10 that connects the internal interface.

```
[S-switch-A] vlan 20
[S-switch-A-vlan20] port GigabitEthernet 0/0/2
[S-switch-A-vlan20] interface vlanif20
[S-switch-A-vlanif20] ip address 202.38.160.1 24
[S-switch-A-vlanif20] vrrp vrid 2 virtual-ip 202.38.160.111
[S-switch-A-vlanif20] vrrp vrid 2 priority 120
[S-switch-A-vlanif20] vrrp vrid 2 track interface GigabitEthernet 0/0/1
reduced 30
```

Create backup group 1 on Vlanif 10 that connects the internal network on S-switch-B. The priority of S-switch-B in backup group 1 is the default value (as the backup router). Backup group 1 tracks Vlanif 20 that connects the external network.

```
<S-switch-B> system-view
[S-switch-B] vlan 10
[S-switch-B-vlan10] port GigabitEthernet 0/0/1
[S-switch-B-vlan10] interface vlanif10
[S-switch-B-vlanif10] ip address 10.1.1.2 24
[S-switch-B-vlanif10] vrrp vrid 1 virtual-ip 10.1.1.111
[S-switch-B-vlanif10] vrrp vrid 1 track interface GigabitEthernet 0/0/2
reduced 30
[S-switch-B-vlanif10] quit
```

Create backup group 2 on Vlanif 20 that connects the external network on S-switch-B. The priority of S-switch-B in backup group 2 is the default value (as the backup router). Backup group 2 tracks Vlanif 10 that connects the internal network.

```
[S-switch-B] vlan 20
[S-switch-B-vlan20] port GigabitEthernet 0/0/2
[S-switch-B-vlan20] interface vlanif20
```

```
[S-switch-B-vlanif20] ip address 202.38.160.2 24
[S-switch-B-vlanif20] vrrp vrid 2 virtual-ip 202.38.160.111
[S-switch-B-vlanif20] vrrp vrid 2 track interface GigabitEthernet 0/0/1
reduced 30
[S-switch-B-vlanif20] quit
```

After the configurations, the interfaces between Host A and Host B can ping through each other.

Running the **display vrrp** command on S-switch-A and S-switch-B, you can view that S-switch-A works in the Master state and S-switch-B works in the Backup state in both backup group 1 and backup group 2.

```
<S-switch-A> display vrrp
vlanif10 | Virtual Router 1
  state : Master
  Virtual IP : 10.1.1.111
  PriorityRun : 120
  PriorityConfig : 120
  MasterPriority : 120
  Preempt : YES    Delay Time : 0
  Timer : 1
  Auth Type : NONE
  Check TTL : YES
  Track IF : vlanif20    Priority reduced : 30
  IF State : UP

vlanif20 | Virtual Router 2
  state : Master
  Virtual IP : 202.38.160.111
  PriorityRun : 120
  PriorityConfig : 120
  MasterPriority : 120
  Preempt : YES    Delay Time : 0
  Timer : 1
  Auth Type : NONE
  Check TTL : YES
  Track IF : vlanif10    Priority reduced : 30
  IF State : UP

<S-switch-B> display vrrp
vlanif10 | Virtual Router 1
  state : Backup
  Virtual IP : 10.1.1.111
  PriorityRun : 100
  PriorityConfig : 100
  MasterPriority : 120
  Preempt : YES    Delay Time : 0
  Timer : 1
  Auth Type : NONE
  Check TTL : YES
  Track IF : vlanif20    Priority reduced : 30
  IF State : UP

vlanif20 | Virtual Router 2
  state : Backup
  Virtual IP : 202.38.160.111
  PriorityRun : 100
  PriorityConfig : 100
  MasterPriority : 120
  Preempt : YES    Delay Time : 0
  Timer : 1
  Auth Type : NONE
  Check TTL : YES
  Track IF : vlanif10    Priority reduced : 30
  IF State : UP
```

3. Configure NAT.

Configure NAT on the interface that connects the external network on S-switch-A. For a packet sent from network segment 10.1.1.0/24, its IP address is translated to that of Vlanif 20.

```
[S-switch-A] acl number 2000
[S-switch-A-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[S-switch-A-acl-basic-2000] quit
[S-switch-A] interface vlanif20/
[S-switch-A-vlanif20] nat outbound 2000
[S-switch-A-vlanif20] quit
```

Configure NAT on the interface that connects the external network on S-switch-B. For a packet sent from network segment 10.1.1.0/24, its IP address is translated to that of Vlanif 20.

```
[S-switch-B] acl number 2000
[S-switch-B-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[S-switch-B-acl-basic-2000] quit
[S-switch-B] interface Vlanif 20
[S-switch-B-vlanif20] nat outbound 2000
[S-switch-B-vlanif20] quit
```

4. Verify the configuration.

After the preceding configuration, Host A can ping through Host B, but Host B cannot ping through Host A.

Configuration File

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
interface GigabitEthernet0/0/1
port default vlan 10
#
interface GigabitEthernet0/0/2
port default vlan 20
#
acl number 2000
rule 5 permit source 10.1.1.0 0.0.0.255
#
interface vlanif10
undo shutdown
ip address 10.1.1.1 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.111
vrrp vrid 1 priority 120
vrrp vrid 1 track interface vlanif20 reduced 30
#
interface vlanif20
undo shutdown
ip address 202.38.160.1 255.255.255.0
nat outbound 2000
vrrp vrid 2 virtual-ip 202.38.160.111
vrrp vrid 2 priority 120
vrrp vrid 2 track interface vlanif10 reduced 30
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 202.38.160.0 0.0.0.255
#
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
interface GigabitEthernet0/0/1
```

```
port default vlan 10
#
interface GigabitEthernet0/0/2
port default vlan 20
#
acl number 2000
rule 5 permit source 10.1.1.0 0.0.0.255
#
interface vlanif10
undo shutdown
ip address 10.1.1.2 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.111
vrrp vrid 1 track interface vlanif20 reduced 30
#
interface vlanif20
undo shutdown
ip address 202.38.160.2 255.255.255.0
nat outbound 2000
vrrp vrid 2 virtual-ip 202.38.160.111
vrrp vrid 2 track interface vlanif10 reduced 30
#
ospf 1
area 0.0.0.0
network 202.38.160.0 0.0.0.255
network 10.1.1.0 0.0.0.255
#
return
```

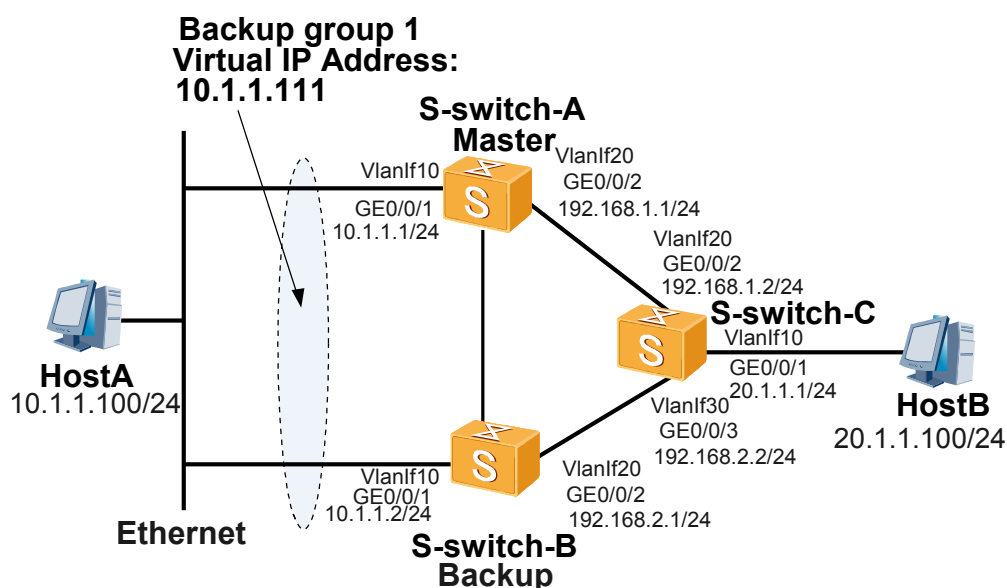
4.9.2 Example for Configuring VRRP in Master/Backup Mode

Networking Requirements

As shown in [Figure 4-3](#), Host A accesses Host B through the default gateway.

The requirements are as follows:

- S-switch-A and S-switch-B form a VRRP backup group that serves as the default gateway for Host B.
- Normally, S-switch-A serves as the gateway. When S-switch-A fails, S-switch-B serves as the gateway.
- S-switch-A continues to function as the master S-switch- within 20 seconds after it recovers.

Figure 4-3 Networking diagram of configuring VRRP in master/backup mode

Configuration Roadmap

The configuration roadmap is as follows:

1. Create backup group 1 S-switch-A and configure S-switch-A with the highest priority in the backup group to be the master S-switch. Configure the preemption mode.
2. Create backup group 1 on GE 0/0/1 interface on S-switch-B and use the default priority.

Data Preparation

To complete the configuration, you need the following data:

- ID of and virtual IP address of the VRRP backup group
- Priority of each S-switch- in the backup group
- Preemption mode

Configuration Procedure

1. Configure network interconnection between devices.
 - # Set the virtual IP address of the default gateway of Host A to 10.1.1.111 and that of the default gateway of Host B to 20.1.1.1.
 - # Set the virtual IP address of the default gateway of Host A to 10.1.1.111 and that of the default gateway of Host B to 20.1.1.1.
 - # Configure S-switch-A, S-switch-B, and S-switch-C to use OSPF for interconnection.
2. Configure VRRP.
 - # On S-switch-A, assign the IP address to the interface, create backup group 1 and set the priority of S-switch-A in this group to 120 (as the master).

```
<S-switch-A> system-view
[S-switch-A] vlan 10
[S-switch-A-vlan10] port GigabitEthernet 0/0/1
[S-switch-A-vlan10] interface vlanif10
[S-switch-A-vlanif10] ip address 10.1.1.1 24
```

```
[S-switch-A-vlanif10] vrrp vrid 1 virtual-ip 10.1.1.111
[S-switch-A-vlanif10] vrrp vrid 1 priority 120
[S-switch-A-vlanif10] vrrp vrid 1 preempt-mode timer delay 20
[S-switch-A-vlanif10] quit
```

On S-switch-B, assign the IP address to the interface, create backup group 1 and set the priority of S-switch-B in this group to the default value (as the backup).

```
<S-switch-B> system-view
[S-switch-B] vlan 10
[S-switch-vlan10] port GigabitEthernet 0/0/1
[S-switch-B-vlan10] interface vlanif10
[S-switch-B-vlanif10] ip address 10.1.1.2 24
[S-switch-B-vlanif10] vrrp vrid 1 virtual-ip 10.1.1.111
[S-switch-B-vlanif10] quit
```

3. Verify the configuration.

- Check that the VRRP backup group can serve as a gateway.

After the previous configuration, Host A can ping through Host B.

Running the **display vrrp** command on S-switch-A, you can view that the status of S-switch-A is **Master**. Running the **display vrrp** command on S-switch-B, you can view that the S-switch-B is **Backup**.

```
<S-switch-A> display vrrp
Vlanif10 | Virtual Router 1
state : Master
Virtual IP : 10.1.1.111
PriorityRun : 120
PriorityConfig : 120
MasterPriority : 120
Preempt : YES   Delay Time : 20
Timer : 1
Auth Type : NONE
Check TTL : YES

<S-switch-B> display vrrp
Vlanif10 | Virtual Router 1
state : Backup
Virtual IP : 10.1.1.111
PriorityRun : 100
PriorityConfig : 100
MasterPriority : 120
Preempt : YES   Delay Time : 0
Timer : 1
Auth Type : NONE
Check TTL : YES
```

Running the **display ip routing-table** command on S-switch-A and S-switch-B, you can view a direct route with the destination address being the virtual IP address on S-switch-A, and an OSPF route to the same destination on S-switch-B.

The displays on S-switch-A and S-switch-B are as follows.

```
<S-switch-A> display ip routing-table
Route Flags: R - relied, D - download to fib
-----
---
Routing Tables: Public
Destinations : 10          Routes : 10
Destination/Mask    Proto Pre  Cost    Flags NextHop          Interface
10.1.1.0/24         Direct 0     0        D  10.1.1.1         Vlanif10
10.1.1.1/32         Direct 0     0        D  127.0.0.1         InLoopBack0
10.1.1.111/32      Direct 0     0        D  127.0.0.1         InLoopBack0
20.1.1.0/24         OSPF   10    2        D  192.168.1.2       Vlanif20
127.0.0.0/8         Direct 0     0        D  127.0.0.1         InLoopBack0
127.0.0.1/32        Direct 0     0        D  127.0.0.1         InLoopBack0
192.168.1.0/24       Direct 0     0        D  192.168.1.1       Vlanif20
192.168.1.1/32       Direct 0     0        D  127.0.0.1         InLoopBack0
192.168.1.2/32       Direct 0     0        D  192.168.1.2       Vlanif20
192.168.2.0/24       OSPF   10    2        D  10.1.1.2          Vlanif10
```

```

<S-switch-B> display ip routing-table
Route Flags: R - relied, D - download to fib
-----
---
Routing Tables: Public
  Destinations : 10          Routes : 10
Destination/Mask    Proto Pre  Cost    Flags NextHop          Interface
10.1.1.0/24         Direct 0     0        D  10.1.1.2          Vlanif10
10.1.1.2/32         Direct 0     0        D  127.0.0.1         InLoopBack0
10.1.1.111/32       OSPF   10    2        D  10.1.1.1          Vlanif10
20.1.1.0/24         OSPF   10    2        D  192.168.2.2       Vlanif20
127.0.0.0/8         Direct 0     0        D  127.0.0.1         InLoopBack0
127.0.0.1/32        Direct 0     0        D  127.0.0.1         InLoopBack0
192.168.1.0/24       OSPF   10    2        D  10.1.1.1          Vlanif10
192.168.2.0/24       Direct 0     0        D  192.168.2.1       Vlanif20
192.168.2.1/32       Direct 0     0        D  127.0.0.1         InLoopBack0
192.168.2.2/32       Direct 0     0        D  192.168.2.2       Vlanif20

```

- Check whether Route B can become the master when S-switch-A fails.

To simulate the selection of the master when S-switch-A fails, run the **shutdown** command on GE 0/0/1 on S-switch-A.

Running the **display vrrp** command on S-switch-B, you can view that S-switch-B is **Master**. The command output is as follows:

```

<S-switch-B> display vrrp
Vlanif10 | Virtual Router 1
  state : Master
  Virtual IP : 10.1.1.111
  PriorityRun : 100
  PriorityConfig : 100
  MasterPriority : 100
  Preempt : YES    Delay Time : 0
  Timer : 1
  Auth Type : NONE
  Check TTL : YES

```

- Check that S-switch-A can perform preemption after recovering.

Run the **undo shutdown** command on GE 0/0/1. On S-switch-A, run the **display vrrp** command to view VRRP status 20 seconds after GE 0/0/1 becomes Up. You can view that S-switch-A restores to be the master.

Configuration Files

- Configuration file of S-switch-A

```

#
sysname S-switch-A
#
interface GigabitEthernet0/0/1
port default vlan 20
#
interface GigabitEthernet0/0/1
port default vlan 10
#
interface Vlanif10
undo shutdown
ip address 10.1.1.1 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.111
vrrp vrid 1 priority 120
vrrp vrid 1 preempt-mode timer delay 20
#
interface Vlanif20
undo shutdown
ip address 192.168.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0

```

```

        network 192.168.1.0 0.0.0.255
        network 10.1.1.0 0.0.0.255
    #
    return

```

- Configuration file of S-switch-B

```

#
sysname S-switch-B
#
interface GigabitEthernet0/0/1
port default vlan 20
#
interface GigabitEthernet0/0/1
port default vlan 10
#
interface Vlanif10
undo shutdown
ip address 10.1.1.2 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.111
#
interface Vlanif20
undo shutdown
ip address 192.168.2.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 192.168.2.0 0.0.0.255
network 10.1.1.0 0.0.0.255
#
return

```

- Configuration file of S-switch-C

```

#
sysname S-switch-C
#
interface GigabitEthernet0/0/1
port default vlan 10
#
interface GigabitEthernet0/0/2
port default vlan 20
#
interface GigabitEthernet0/0/3
port default vlan 30
#
interface Vlanif10
undo shutdown
ip address 20.1.1.1 255.255.255.0
#
interface Vlanif20
undo shutdown
clock master
ip address 192.168.1.2 255.255.255.0
#
interface Vlanif30
undo shutdown
clock master
ip address 192.168.2.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
network 192.168.2.0 0.0.0.255
network 20.1.1.0 0.0.0.255
#
return

```

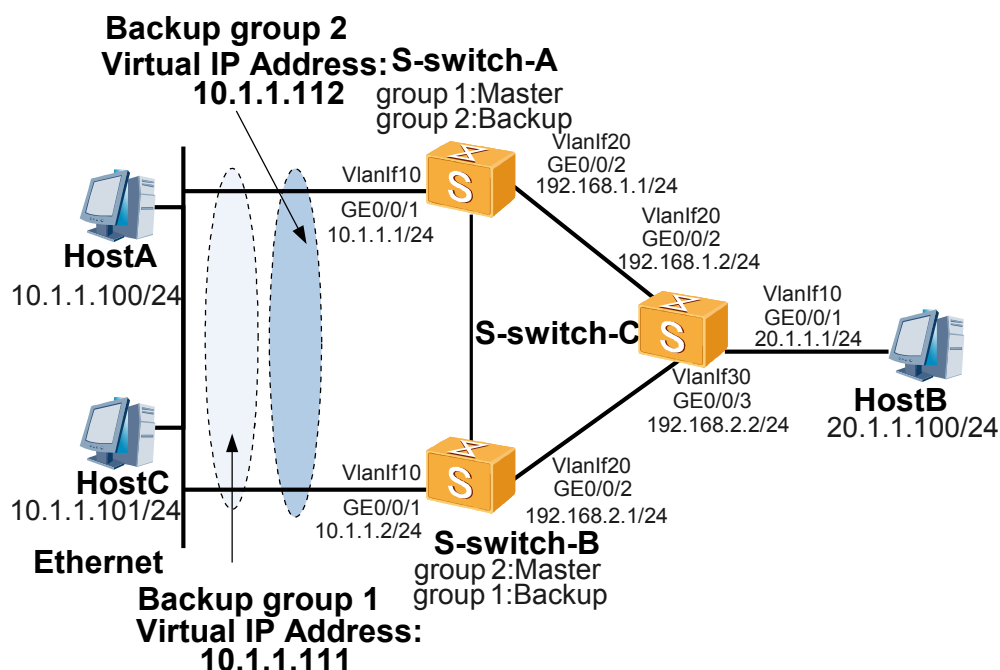
4.9.3 Example for Configuring VRRP in Load Balancing Mode

Networking Requirements

As shown in [Figure 4-4](#).

- S-switch-A serves as the master of group 1 and the backup of group 2.
- S-switch-B serves as the master of backup group 2 and the backup of group 1.
- Host A in the internal network takes backup group 1 as its gateway and Host C takes backup group 2 as its gateway to share the traffic and backup each other.

Figure 4-4 Networking diagram of configuring VRRP in load balancing mode



Configuration Roadmap

The configuration roadmap is as follows:

1. Create two backup groups on S-switch-A. S-switch-A is the master in backup group 1 and the backup S-switch in backup group 2.
2. Create two backup groups on S-switch-B. S-switch-B is the backup in backup group 1 and the master in backup group 2.

Data Preparation

To complete the configuration, you need the following data:

- Virtual router IDs and virtual IP addresses
- Priority of each S-switch in the backup groups

Configuration Procedure

1. Configure the network interconnection between devices.

Set the virtual IP address of the default gateway of Host A to 10.1.1.111 in backup group 1, that of the default gateway of Host B to 20.1.1.1, and that of the default gateway of Host C to 10.1.1.112 in backup group 2.

Configure S-switch-A, S-switch-B, and S-switch-C to use OSPF for interconnection.

2. Configure VRRP.

On S-switch-A, assign an IP address to the interface, create backup group 1, and set the priority of S-switch-A in this group to 120 (as the master). Create backup group 2 and set the priority of S-switch-A in this group to the default value 100 (as the backup).

```
<S-switch-A> system-view
[S-switch-A] vlan 10
[S-switch-A-vlan10] port GigabitEthernet 0/0/1
[S-switch-A-vlan10] interface vlanif10
[S-switch-A-vlanif10] ip address 10.1.1.1 24
[S-switch-A-vlanif10] vrrp vrid 1 virtual-ip 10.1.1.111
[S-switch-A-vlanif10] vrrp vrid 1 priority 120
[S-switch-A-vlanif10] vrrp vrid 2 virtual-ip 10.1.1.112
[S-switch-A-vlanif10] quit
```

On S-switch-B, assign an IP address to the interface, create backup group 1 and set the priority of S-switch-B in this group to the default value 100 (as the backup). Create backup group 2, and set the priority of S-switch-B in this group to 120 (as the master).

```
<S-switch-B> system-view
[S-switch-B] vlan 10
[S-switch-B-vlan10] port GigabitEthernet 0/0/1
[S-switch-B-vlan10] interface vlanif10
[S-switch-B-vlanif10] ip address 10.1.1.2 24
[S-switch-B-vlanif10] vrrp vrid 1 virtual-ip 10.1.1.111
[S-switch-B-vlanif10] vrrp vrid 2 virtual-ip 10.1.1.112
[S-switch-B-vlanif10] vrrp vrid 2 priority 120
[S-switch-B-vlanif10] quit
```

3. Verify the configuration.

After the previous configuration, Host A and Host C in the network can ping through Host B.

Tracert Host B from Host A and Host C. Packets from Host A to Host B pass through S-switch-A and S-switch-C. Packets from Host C to Host B pass through S-switch-A and S-switch-C. That is, load balancing is enabled on S-switch-A and S-switch-B to share the internal traffic.

```
<HostA> tracert 20.1.1.100
tracert to 20.1.1.100(20.1.1.100) 30 hops max, 40 bytes packet
 1 10.1.1.1 120 ms 50 ms 60 ms
 2 192.168.1.2 100 ms 60 ms 60 ms
 3 20.1.1.100 130 ms 90 ms 90 ms
<HostC> tracert 20.1.1.100
tracert to 20.1.1.100(20.1.1.100) 30 hops max, 40 bytes packet
 1 10.1.1.2 30 ms 60 ms 40 ms
 2 192.168.2.2 90 ms 60 ms 60 ms
 3 20.1.1.100 70 ms 60 ms 90 ms
```

Running the **display vrrp** command on S-switch-A, you can view that S-switch-A serves as the master in backup group 1 and the backup in backup group 2.

```
<S-switch-A> display vrrp
vlanif10 | Virtual Router 1
state : Master
Virtual IP : 10.1.1.111
PriorityRun : 120
PriorityConfig : 120
MasterPriority : 120
Preempt : YES Delay Time : 0
Timer : 1
Auth Type : NONE
Check TTL : YES
```

```

vlanif10 | Virtual Router 2
state : Backup
Virtual IP : 10.1.1.112
PriorityRun : 100
PriorityConfig : 100
MasterPriority : 120
Preempt : YES    Delay Time : 0
Timer : 1
Auth Type : NONE
Check TTL : YES

```

Configuration Files

- Configuration file of S-switch-A

```

#
sysname S-switch-A
#
interface GigabitEthernet0/0/1
port default vlan 20
#
interface GigabitEthernet0/0/1
port default vlan 10
#
interface vlanif10
undo shutdown
ip address 10.1.1.1 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.111
vrrp vrid 1 priority 120
vrrp vrid 2 virtual-ip 10.1.1.112
#
interface vlanif20
undo shutdown
ip address 192.168.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
network 10.1.1.0 0.0.0.255
#
return

```

- Configuration file of S-switch-B

```

#
sysname S-switch-B
#
interface GigabitEthernet0/0/1
port default vlan 20
#
interface GigabitEthernet0/0/1
port default vlan 10
#
interface vlanif10
undo shutdown
ip address 10.1.1.2 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.111
vrrp vrid 2 virtual-ip 10.1.1.112
vrrp vrid 2 priority 120
#
interface vlanif20
undo shutdown
ip address 192.168.2.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 192.168.2.0 0.0.0.255
network 10.1.1.0 0.0.0.255
#
return

```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
interface GigabitEthernet0/0/1
port default vlan 10
#
interface GigabitEthernet0/0/2
port default vlan 20
#
interface GigabitEthernet0/0/3
port default vlan 30
#
interface Vlanif10
undo shutdown
ip address 20.1.1.1 255.255.255.0
#
interface Vlanif20
undo shutdown
ip address 192.168.1.2 255.255.255.0
#
interface Vlanif30
undo shutdown
ip address 192.168.2.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
network 192.168.2.0 0.0.0.255
network 20.1.1.0 0.0.0.255
#
return
```