



Quidway S5300 Series Ethernet Switches
V100R002C02

Configuration Guide - Network Management

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 SNMP Configuration.....	1-1
1.1 Introduction to SNMP.....	1-2
1.1.1 SNMP Architecture.....	1-2
1.1.2 SNMP Operation Process.....	1-2
1.1.3 MIB.....	1-3
1.1.4 Logical Relationships Between Configuration Tasks.....	1-4
1.2 Configuring SNMP.....	1-4
1.2.1 Establishing the Configuration Task.....	1-4
1.2.2 Configuring Basic SNMP Agent Functions.....	1-5
1.2.3 Setting an SNMP Community Name.....	1-5
1.2.4 Configuring the SNMP Group and Users.....	1-6
1.2.5 Configuring Information About the MIB View.....	1-6
1.2.6 Configuring the Maximum Length of SNMP Packets.....	1-6
1.2.7 Checking the Configuration.....	1-7
1.3 Configuring the Trap Function.....	1-7
1.3.1 Establishing the Configuration Task.....	1-8
1.3.2 Enabling the Device to Send Trap Messages.....	1-8
1.3.3 Setting the Destination Host of Trap Messages.....	1-8
1.3.4 Setting the Source Address of Trap Messages.....	1-9
1.3.5 Setting the Queue Length of Trap Messages.....	1-9
1.3.6 Setting the Saving Time of Trap Messages.....	1-9
1.3.7 Checking the Configuration.....	1-9
1.4 Maintaining SNMP.....	1-10
1.5 Configuration Examples.....	1-10
1.5.1 Example for Configuring an NMS to Manage the S-switch Through the In-Band Mode.....	1-10
2 RMON Configuration.....	2-1
2.1 Introduction to RMON.....	2-2
2.1.1 RMON.....	2-2
2.1.2 Implementing RMON on the S-switch.....	2-2
2.1.3 Logical Relationships Between Configuration Tasks.....	2-4
2.2 Configuring the RMON Statistics Function.....	2-4

2.2.1 Establishing the Configuration Task.....	2-5
2.2.2 Enabling the RMON Statistics Function on an Interface.....	2-5
2.2.3 (Optional) Configuring the etherStatsTable.....	2-6
2.2.4 (Optional) Configuring the historyControlTable.....	2-6
2.2.5 Checking the Configuration.....	2-7
2.3 Configuring the RMON Alarm Function.....	2-7
2.3.1 Establishing the Configuration Task.....	2-7
2.3.2 Configuring the eventTable.....	2-8
2.3.3 (Optional) Configuring the alarmTable.....	2-8
2.3.4 (Optional) Configuring the priAlarmTable.....	2-9
2.3.5 Checking the Configuration.....	2-10
2.4 Maintaining RMON.....	2-10
2.5 Configuration Examples.....	2-11
2.5.1 Examples for Configuring RMON.....	2-11
3 HGMP Configuration.....	3-1
3.1 Introduction.....	3-3
3.1.1 HGMP.....	3-3
3.1.2 NDP.....	3-3
3.1.3 NTDP.....	3-4
3.1.4 Roles in a Cluster.....	3-4
3.1.5 Delivery in Batches.....	3-4
3.1.6 Batch Restart.....	3-5
3.1.7 Incremental Configuration.....	3-5
3.1.8 Synchronization of Configuration Files.....	3-5
3.1.9 Security Features.....	3-5
3.1.10 Plug-and-play Function.....	3-6
3.1.11 Logical Relationships Between Configuration Tasks.....	3-6
3.2 Configuring NDP.....	3-6
3.2.1 Establishing the Configuration Task.....	3-7
3.2.2 Enabling NDP.....	3-7
3.2.3 (Optional) Configuring the Holding Time of NDP Packets.....	3-8
3.2.4 (Optional) Setting the Interval for Sending NDP Packets.....	3-8
3.2.5 Checking the Configuration.....	3-9
3.3 Configuring NTDP.....	3-9
3.3.1 Establishing the Configuration Task.....	3-10
3.3.2 Enabling NTDP.....	3-10
3.3.3 (Optional) Configuring the Topology Collection Range.....	3-11
3.3.4 (Optional) Configuring the Delay for Forwarding NTDP Packets.....	3-11
3.3.5 (Optional) Configuring the Interval for Collecting Topology Information.....	3-12
3.3.6 (Optional) Enabling Topology Information Collection.....	3-12
3.3.7 Checking the Configuration.....	3-12
3.4 Configuring a Cluster.....	3-13

3.4.1 Establishing the Configuration Task.....	3-13
3.4.2 Configuring a Management VLAN.....	3-14
3.4.3 Enabling the Cluster Function.....	3-15
3.4.4 Creating a Cluster.....	3-15
3.4.5 Checking the Configuration.....	3-16
3.5 Deleting or Quitting a Cluster.....	3-17
3.5.1 Establishing the Configuration Task.....	3-17
3.5.2 Deleting a Cluster.....	3-18
3.5.3 Quitting a Cluster.....	3-18
3.5.4 Checking the Configuration.....	3-18
3.6 Adding a Member Switch.....	3-19
3.6.1 Establishing the Configuration Task.....	3-19
3.6.2 Adding a Member Switch.....	3-19
3.6.3 Checking the Configuration.....	3-20
3.7 Deleting a Member Switch.....	3-20
3.7.1 Establishing the Configuration Task.....	3-21
3.7.2 Deleting a Member Switch.....	3-21
3.7.3 Checking the Configuration.....	3-21
3.8 Setting Parameters for a Cluster.....	3-22
3.8.1 Configuring the Interval for Sending Handshake Packets.....	3-22
3.8.2 Configuring the Holdtime of Handshake Packets.....	3-22
3.8.3 Enabling Candidate Switches to Join a Cluster Automatically.....	3-23
3.8.4 Setting the Aging Time of Member Switches.....	3-23
3.8.5 Configuring a Multicast Address for a Cluster.....	3-23
3.8.6 Configuring the Mode for Interfaces in the Cluster to Join a VLAN.....	3-24
3.8.7 Configuring the Pubic Server and Host.....	3-24
3.9 Maintaining HGMP.....	3-25
3.9.1 Clearing the Statistics of NDP.....	3-25
3.9.2 Debugging NDP.....	3-25
3.9.3 Debugging NTDP.....	3-26
3.9.4 Debugging a Cluster.....	3-26
3.10 Adjusting Cluster Parameters.....	3-26
3.10.1 Establishing the Configuration Task.....	3-27
3.10.2 Configuring the Interval for Sending Handshake Packets.....	3-28
3.10.3 Configuring the Holdtime of Packets.....	3-28
3.10.4 Enabling Candidate Switches to Join a Cluster Automatically.....	3-28
3.10.5 Setting the Aging Time of Member Switches.....	3-29
3.10.6 Configuring a Multicast Address for a Cluster.....	3-29
3.10.7 Configuring the Mode for Interfaces in the Cluster to Join a VLAN.....	3-29
3.10.8 Configuring Public Servers and Hosts for a Cluster.....	3-30
3.10.9 Checking the Configuration.....	3-30
3.11 Managing Switches in a Cluster Through HGMP.....	3-31

3.11.1 Establishing the Configuration Task.....	3-31
3.11.2 Sending Files to Member Switches in a Cluster in Batches.....	3-32
3.11.3 Restarting Member Switches in a Cluster in Batches.....	3-32
3.11.4 Enabling the Plug-and-Play Function.....	3-33
3.11.5 Sending the Incremental Configuration.....	3-33
3.11.6 Synchronizing Configuration Files.....	3-34
3.11.7 Configuring Security Features.....	3-34
3.11.8 Checking the Configuration.....	3-35
3.12 Configuration Examples.....	3-36
3.12.1 Example for Creating a Cluster.....	3-36
3.12.2 Example for Member Switches Accessing a Public FTP Server Through FTP.....	3-43
3.12.3 Example for Devices Outside the Cluster Accessing Member Switches Through FTP.....	3-44
3.12.4 Example for Sending Files to Member Switches in a Cluster in Batches.....	3-46
3.12.5 Example for Restarting Member Switches in a Cluster in Batches.....	3-51
3.12.6 Example for Configuring the Incremental Configuration.....	3-55
3.12.7 Example for Synchronizing Configuration Files.....	3-60
3.12.8 Example for Configuring Security Features.....	3-64
4 LLDP Configuration.....	4-1
4.1 Introduction.....	4-2
4.1.1 LLDP Overview.....	4-2
4.1.2 Basic Concepts.....	4-3
4.1.3 Logical Relationships Between Configuration Tasks.....	4-4
4.2 Configuring LLDP.....	4-4
4.2.1 Establishing the Configuration Task.....	4-4
4.2.2 (Optional) Enabling the LLDP Trap Function.....	4-6
4.2.3 Enabling LLDP on an Interface.....	4-6
4.2.4 (Optional) Disabling LLDP on an Interface.....	4-7
4.2.5 (Optional) Re-enabling LLDP on an Interface.....	4-7
4.2.6 (Optional) Setting the LLDP Management Address.....	4-7
4.2.7 (Optional) Setting LLDP Attributes.....	4-8
4.2.8 Checking the Configuration.....	4-10
4.3 Maintaining LLDP.....	4-14
4.3.1 Clearing the LLDP Statistics.....	4-14
4.3.2 Monitoring the Running Status of LLDP.....	4-15
4.4 Configuration Examples.....	4-15
4.4.1 Example for Configuring LLDP.....	4-15
4.4.2 Example for Configuring LLDP on the Network an Eth-Trunk.....	4-18
5 NQA Configuration.....	5-1
5.1 Introduction.....	5-3
5.1.1 Overview of NQA.....	5-3
5.1.2 Comparisons Between NQA and Ping.....	5-3
5.1.3 NQA Client and NQA Server.....	5-4

5.1.4 NQA Features Supported by the S-switch.....	5-4
5.2 Configuring an ICMP Test.....	5-5
5.2.1 Establishing the Configuration Task.....	5-6
5.2.2 Configuring ICMP Test Parameters.....	5-6
5.2.3 Checking the Configuration.....	5-7
5.3 Configuring a DHCP Test.....	5-8
5.3.1 Establishing the Configuration Task.....	5-9
5.3.2 Configuring DHCP Test Parameters.....	5-9
5.3.3 Checking the Configuration.....	5-10
5.4 Configuring the FTP Download Test.....	5-11
5.4.1 Establishing Configuration Tasks.....	5-11
5.4.2 Configuring the FTP Download Test Parameters.....	5-12
5.4.3 Checking the Configuration.....	5-13
5.5 Configuring an FTP Upload Test.....	5-14
5.5.1 Establishing the Configuration Tasks.....	5-14
5.5.2 Configuring the FTP Upload Test Parameters.....	5-15
5.5.3 Checking the Configuration.....	5-16
5.6 Configuring an HTTP Test.....	5-17
5.6.1 Establishing the Configuration Task.....	5-17
5.6.2 Configuring the HTTP Test Parameters.....	5-18
5.6.3 Checking the Configuration.....	5-19
5.7 Configuring the SNMP Query Test.....	5-20
5.7.1 Establishing the Configuration Task.....	5-21
5.7.2 Setting Parameters for the SNMP Query Test.....	5-21
5.7.3 Checking the Configuration.....	5-22
5.8 Configuring a TCP Test.....	5-23
5.8.1 Establishing the Configuration Task.....	5-23
5.8.2 Configuring the TCP Server.....	5-24
5.8.3 Configuring the TCP Client.....	5-24
5.8.4 Checking the Configuration.....	5-25
5.9 Configuring a UDP Test.....	5-26
5.9.1 Establishing the Configuration Task.....	5-26
5.9.2 Configuring the UDP Server.....	5-27
5.9.3 Configuring the UDP Client.....	5-27
5.9.4 Checking the Configuration.....	5-28
5.10 Configuring a Jitter Test.....	5-29
5.10.1 Establishing the Configuration Task.....	5-29
5.10.2 Configuring the Jitter Server.....	5-30
5.10.3 Configuring the Jitter Client.....	5-31
5.10.4 Checking the Configuration.....	5-32
5.11 Configuring an NQA Test Group.....	5-33
5.11.1 Establishing the Configuration Task.....	5-33

5.11.2 Configuring an NQA Test Group.....	5-34
5.11.3 Checking the Configuration.....	5-35
5.12 Configuring Universal NQA Test Parameters.....	5-36
5.12.1 Establishing the Configuration Task.....	5-36
5.12.2 Configuring the Universal NQA Test Parameters.....	5-37
5.12.3 Checking the Configuration.....	5-37
5.13 Configuring the Bidirectional Transmission Delay Threshold.....	5-38
5.13.1 Establishing the Configuration Task.....	5-38
5.13.2 Configuring the Bidirectional Transmission Delay Threshold.....	5-38
5.13.3 Checking the Configuration.....	5-39
5.14 Configuring the Unidirectional Transmission Delay Threshold.....	5-39
5.14.1 Establishing the Configuration Task.....	5-40
5.14.2 Configuring the Unidirectional Transmission Delay Threshold.....	5-40
5.14.3 Checking the Configuration.....	5-41
5.15 Configuring the Trap Function.....	5-41
5.15.1 Establishing the Configuration Task.....	5-41
5.15.2 Enabling the Trap Function for Test Failures.....	5-43
5.15.3 Enabling the Trap Function for Probe Failures.....	5-43
5.15.4 Enabling the Trap Function for Probe Successes.....	5-43
5.15.5 Enabling the Trap Function When the Transmission Delay Exceeds the Threshold.....	5-44
5.15.6 Checking the Configuration.....	5-44
5.16 Maintaining NQA.....	5-44
5.16.1 Restarting an NQA Test Instance.....	5-45
5.16.2 Clearing NQA Statistics.....	5-45
5.16.3 Debugging NQA.....	5-45
5.17 Configuration Examples.....	5-46
5.17.1 Example for Configuring the ICMP Test.....	5-46
5.17.2 Example for Configuring the DHCP Test.....	5-48
5.17.3 Example for Configuring an FTP Download Test.....	5-49
5.17.4 Example for Configuring an FTP Upload Test.....	5-51
5.17.5 Example for Configuring the HTTP Test.....	5-54
5.17.6 Example for Configuring the SNMP Query Test.....	5-56
5.17.7 Example for Configuring a TCP Test.....	5-58
5.17.8 Example for Configuring the UDP Test.....	5-60
5.17.9 Example for Configuring a Jitter Test.....	5-62
5.17.10 Example for Configuring an NQA Test Group.....	5-65
5.17.11 Example for Enabling the Trap Function When the Transmission Delay Exceeds the Threshold	5-68

Figures

Figure 1-1 SNMP architecture.....	1-2
Figure 1-2 MIB tree structure.....	1-4
Figure 1-3 Typical networking of configuring an NMS to manage the S-switch through the in-band mode	1-11
Figure 2-1 Figure 2-1 Networking diagram of configuring RMON.....	2-11
Figure 3-1 Networking diagram for creating a cluster.....	3-37
Figure 3-2 Networking diagram for accessing a public FTP server.....	3-43
Figure 3-3 Networking diagram for devices accessing S-switch-C through FTP.....	3-45
Figure 3-4 Networking diagram for sending files to member switches in a cluster in batches.....	3-47
Figure 3-5 Networking diagram for restarting member switches in a cluster in batches.....	3-52
Figure 3-6 Networking diagram for configuring the incremental configuration function for an HGMP cluster	3-56
Figure 3-7 Networking diagram for synchronizing configuration files for an HGMP cluster.....	3-60
Figure 3-8 Networking diagram for configuring security features for an HGMP cluster.....	3-65
Figure 4-1 Networking diagram of LLDP application.....	4-5
Figure 4-2 Networking for configuring LLDP.....	4-16
Figure 4-3 Networking for configuring LLDP on the network with an Eth-Trunk.....	4-19
Figure 5-1 Diagram of an NQA test.....	5-3
Figure 5-2 Relationships between the NQA client and the NQA server.....	5-4
Figure 5-3 Networking diagram of the ICMP test.....	5-47
Figure 5-4 Networking diagram of the DHCP test.....	5-48
Figure 5-5 Networking diagram of the FTP test.....	5-50
Figure 5-6 Networking diagram of the FTP test.....	5-52
Figure 5-7 Networking diagram of the HTTP test.....	5-54
Figure 5-8 Networking diagram of the SNMP Query test.....	5-56
Figure 5-9 Networking diagram of the TCP test.....	5-58
Figure 5-10 Networking diagram of the UDP test.....	5-60
Figure 5-11 Networking diagram of a jitter test.....	5-62
Figure 5-12 Networking diagram of an NQA test group.....	5-65
Figure 5-13 Networking diagram of enabling the trap function when the transmission delay exceeds the threshold	5-68

Tables

Table 1-1 Basic SNMP operations..... 1-3

Table 2-1 Capacity of the table and TTL..... 2-4

About This Document

Purpose

This document describes the device management features that are supported by the S-switch by providing configuration procedures and configuration examples.

This document covers the following topics:

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

This document can instruct you in the methods of configuring these network management features and the scenarios to which these network management features should apply.

Version

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 engineer
- Network monitoring engineer
- System maintenance engineers

Organization





This document is organized as follows.


Chapter	Description
1 SNMP Configuration	Describes the basics of the Simple Network Management Protocol (SNMP) and the procedure for configuring SNMP, trap functions, interface index features, and maintaining SNMP. Provides configuration examples and troubleshooting.
2 RMON Configuration	Describes the basics of Remote Monitoring (RMON) and the procedures for configuring RMON.
3 HGMP Configuration	Describes the basics of the Huawei Group Management Protocol (HGMP) and the procedures for configuring the Neighbor Discovery Protocol (NDP), Network Topology Discovery Protocol (NTDP), and cluster.
4 LLDP Configuration	Describes the basics of Link Layer Discovery Protocol (LLDP) and the procedures for configuring LLDP.
5 NQA Configuration	Describes the basics of NQA and the procedures for configuring NQA.

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 injuries.
 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 solve a problem or save you time.

Symbol	Description
 NOTE	Indicates additional information to emphasize or supplement important points of the main text.

General Conventions

Conventions	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Boldface	Names of files, directories, folders, and users are in boldface .
<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

Conventions	Description
Boldface	The keywords of a command line are in boldface .
<i>Italic</i>	Command arguments are in <i>italic</i> .
[]	Items (keywords or arguments) in brackets [] are optional.
{ x y ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x y ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none 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 alternative items are grouped in square brackets and separated by vertical bars. Several or none is 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

Conventions	Description
“ ”	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 FileCreate > Folder > .

Keyboard Operations

Conventions	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

Conventions	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.

Revision History

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

Updates in Issue 01 (12.26.08)

This is the first release.

1 SNMP Configuration

About This Chapter

This chapter describes the basics of the Simple Network Management Protocol (SNMP) and the procedure for configuring SNMP, trap functions, interface index features, and maintaining SNMP. This chapter also provides configuration examples and troubleshooting of SNMP.

Context

[1.1 Introduction to SNMP](#)

This section describes the architecture and operation process of SNMP.

[1.2 Configuring SNMP](#)

This section describes how to configure SNMP.

[1.3 Configuring the Trap Function](#)

This section describes how the device sends a trap message to the NMS without any request to report an urgent and important event.

[1.4 Maintaining SNMP](#)

This section describes how to maintain SNMP.

[1.5 Configuration Examples](#)

This section provides several examples of SNMP.

1.1 Introduction to SNMP

This section describes the architecture and operation process of SNMP.

1.1.1 SNMP Architecture

1.1.2 SNMP Operation Process

1.1.3 MIB

1.1.4 Logical Relationships Between Configuration Tasks

1.1.1 SNMP Architecture

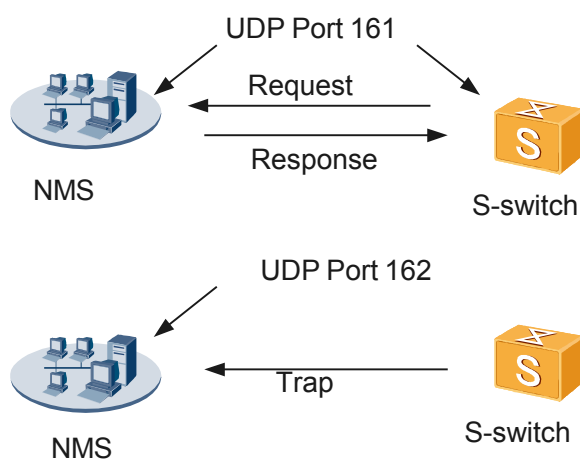
The SNMP architecture consists of the Network Management Station (NMS) and the Agent. SNMP is an application layer protocol that defines the transmission of management information between the NMS and the Agent.

The NMS is a workstation on which the server program runs. The popular network management platforms are Sun NetManager and IBM NetView. An NMS sends various types of query packets to network devices, receives response packets and trap messages from the managed devices, and displays the results.

The agent is a process performed on the managed devices. The Agent receives and processes the request packets from the NMS and read or write management variables according to the type of packets. Then, the Agent sends response packets to the NMS. In the case of an abnormal event, such as the startup of the device, the agent sends a trap message to the NMS.

Figure 1-1 shows the relationship between the NMS and Agent.

Figure 1-1 SNMP architecture



1.1.2 SNMP Operation Process

The Agent on the S-switch receives request packets from the NMS through UDP port 161. After decoding the packets and authenticating the community name of the packets, the Agent obtains the corresponding nodes of management variables in the Management Information Base (MIB)

tree. The Agent also obtains the values of management variables from the corresponding modules. The agent then sends an encoded response packet to the NMS. After receiving the response packet, the NMS decodes the packet and authenticates the community name of the packet. Finally, the result is displayed.

The agent processes the received packet as follows:

1. Decodes the packet based on the ASN.1 basic encoding rule and generates the packet represented in the internal data structure. The Agent discards the packet if the decoding fails.
2. Obtains the version number from the packet. The Agent discards the packet if the version is inconsistent with the SNMP version supported by the Agent.
3. Obtains the community name from the packet which is filled in by the NMS that sends the packet. If the community name is inconsistent with what the agent accepts, the agent discards the packet. At the same time, a trap message is sent to the NMS. SNMPv1 provides a relatively weak security measure, but the security measure supported by SNMPv3 is greatly enhanced.
4. Gets a Protocol Data Unit (PDU) from the authenticated ASN.1 object. If the operation fails, the agent discards the packet. Otherwise, the agent processes the PDU to generate another packet, whose destination address is the same as the source address of the received packet.

SNMP processes each PDU in a different manner.

SNMP substitutes the Get-set mode for a complex command set and uses basic operations to complete all operations. In addition, you can adopt the MIB standard or standard mode to define your own MIB. This reduces the cost of the entire network management by reducing the cost of most agent components in the NMS.

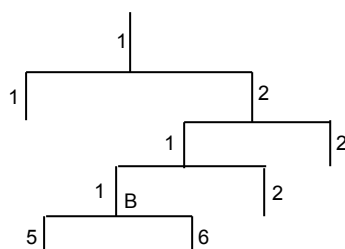
Table 1-1 lists basic SNMP operations.

Table 1-1 Basic SNMP operations

Action	Command
Get-request	Obtains a value from a variable.
Get-next-request	Obtains the next value from the table.
Get-response	Responds to the Get operation.
Set-request	Saves a value to a specific variable.
Trap	Reports a trap message about the event.

1.1.3 MIB

To uniquely identify a management variable, SNMP uses a hierarchical naming method to distinguish between managed objects. This hierarchical structure is like a tree with the nodes representing managed objects. **Figure 1-2** shows a managed object that can be identified by the path from the root to the node representing it.

Figure 1-2 MIB tree structure

As shown in the preceding figure, the managed object B can be determined by a string of digits {1.2.1.1}. This string is its object identifier. The MIB, which describes the hierarchical structure of the tree, is a collection of standard variables on monitored network devices.

Currently, the SNMP agent on the S-switch supports SNMPv3 and is compatible with SNMPv1 and SNMPv2c.

For details on the MIBs supported by the S-switch, refer to the *Quidway S5300 Series Ethernet Switches MIB Reference*.

1.1.4 Logical Relationships Between Configuration Tasks

Before performing the task of **1.3 Configuring the Trap Function**, you must perform the task of **1.2 Configuring SNMP**.

1.2 Configuring SNMP

This section describes how to configure SNMP.

1.2.1 Establishing the Configuration Task

1.2.2 Configuring Basic SNMP Agent Functions

1.2.3 Setting an SNMP Community Name

1.2.4 Configuring the SNMP Group and Users

1.2.5 Configuring Information About the MIB View

1.2.6 Configuring the Maximum Length of SNMP Packets

1.2.7 Checking the Configuration

1.2.1 Establishing the Configuration Task

Applicable Environment

The S-switch is configured as an SNMP agent to process request packets sent from an NMS and return response packets.

Pre-configuration Tasks

Before configuring SNMP, complete the following tasks:

- Configuring the network layer address of the S-switch

- Configuring a reachable route between the S-switch and NMS

Data Preparation

To configure SNMP, you need the following data.

No.	Data
1	SNMP version and system information
2	SNMP community name
3	SNMP group name and contained users

1.2.2 Configuring Basic SNMP Agent Functions

Context

After the device is enabled as an SNMP agent, the system automatically configures the SNMP version (SNMPv3) and the engine ID of the local SNMP entity.

The engine ID of the local SNMP entity is a hexadecimal numerical string. The default value is the enterprise number plus the device information. The device information can be an IP address, a MAC address, or a user-defined hexadecimal numerical string.

contact (system contact) is a management variable of the system group in MIB II. It contains the identification and contact information about relevant administrators of the managed device. By configuring this parameter, you can store the information in the S-switch for query.

location is a management variable of the system group in the MIB and stands for the location of a managed device.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
 - Step 2** Run the **snmp-agent** command to configure the device as an SNMP agent.
 - Step 3** Run the **snmp-agent sys-info version { { v1 | v2c | v3 } * | all }** command to set the SNMP version.
 - Step 4** Run the **snmp-agent local-engineid *engineid*** command to set an engine ID for the local SNMP entity.
 - Step 5** (Optional) Run the **snmp-agent sys-info contact *contact*** command to set the contact information about the administrator.
 - Step 6** (Optional) Run the **snmp-agent sys-info location *location*** command to set the location of the S-switch.
- End

1.2.3 Setting an SNMP Community Name

Context

SNMPv1 and SNMPv2c use community names for authentication. SNMP packets that do not match the authenticated community name of the device are discarded.

An SNMP community is named with a character string called the community name. Communities have different access rights such as read-only and read-write. The community with the read-only right can only query information about the device, whereas the community with the read-write right can also configure the device.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **snmp-agent community { read | write } community-name [[acl acl-number]] [mib-view view-name]] *** command to set the community name and access authority.
- End

1.2.4 Configuring the SNMP Group and Users

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **snmp-agent group v3 group-name [authentication | privacy] [read-view read-view] [write-view write-view] [notify-view notify-view] [acl acl-number]** command to set the SNMPv3 group.
- Step 3** Run the **snmp-agent usm-user v3 user-name group-name [[authentication-mode { md5 | sha } auth-password] [privacy-mode des56 priv-password]] [acl acl-number]** command to add a user to the SNMPv3 group.
- End

1.2.5 Configuring Information About the MIB View

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **snmp-agent mib-view { excluded | included } view-name oid-tree** command to configure information about the MIB view.
- End

1.2.6 Configuring the Maximum Length of SNMP Packets

Procedure

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

Step 2 Run the **snmp-agent packet max-size** *size* command to set the maximum length of SNMP packets that the agent can receive and send.

----End

1.2.7 Checking the Configuration

Context

Run the following commands to check the previous configuration.

Action	Command
Check the statistics about SNMP packets.	display snmp-agent statistics
Check the engine ID of the current device.	display snmp-agent { local-engineid remote-engineid }
Check the names, security modes, status of various MIB views, and storage modes of SNMP groups.	display snmp-agent group [group-name]
Check the names of all SNMPv3 users.	display snmp-agent usm-user [engineid engineid group group-name username user-name] *
Check the currently configured community names.	display snmp-agent community [read write]
Check the currently configured MIB view.	display snmp-agent mib-view [exclude include viewname view-name]
Check the contact information used for system maintenance, which is a string of characters.	display snmp-agent sys-info contact
Check the location of the system, which is a string of characters.	display snmp-agent sys-info location
Check the information about the SNMP version.	display snmp-agent sys-info version

1.3 Configuring the Trap Function

This section describes how the device sends a trap message to the NMS without any request to report an urgent and important event.

[1.3.1 Establishing the Configuration Task](#)

[1.3.2 Enabling the Device to Send Trap Messages](#)

[1.3.3 Setting the Destination Host of Trap Messages](#)

[1.3.4 Setting the Source Address of Trap Messages](#)

[1.3.5 Setting the Queue Length of Trap Messages](#)

[1.3.6 Setting the Saving Time of Trap Messages](#)[1.3.7 Checking the Configuration](#)

1.3.1 Establishing the Configuration Task

Applicable Environment

A trap message that reports an urgent and important event is sent to the NMS by a managed device without any request. You must configure the trap function before enabling the S-switch to send trap messages.

Pre-configuration Tasks

Before configuring the trap function, complete the following tasks:

- Configuring the network layer address of the S-switch
- Configuring a reachable route existing between the S-switch and the trap host

Data Preparation

To configure the trap function, you need the following data.

No.	Data
1	Destination host address of trap messages
2	Source address of trap messages
3	Queue length and saving time of trap messages

1.3.2 Enabling the Device to Send Trap Messages

Procedure

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

Step 2 Run the **snmp-agent trap enable [trap-type [trap-list]]** command to enable the device to send trap messages.

If no parameter is specified, trap messages of all types and all modules can be sent.

----End

1.3.3 Setting the Destination Host of Trap Messages

Procedure

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

- Step 2** Run the **snmp-agent target-host trap address udp-domain** *ip-address* [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]] command to set the destination host of trap messages.

----End

1.3.4 Setting the Source Address of Trap Messages

Procedure

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

- Step 2** Run the **snmp-agent trap source** *interface-type interface-number* command to set the source address of trap messages.



NOTE

Only an interface with an IP address can be set as the source address.

You can use this command to set or delete the source address of the interface that sends trap messages.

----End

1.3.5 Setting the Queue Length of Trap Messages

Procedure

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

- Step 2** Run the **snmp-agent trap queue-size** *size* command to set the queue length of trap messages.

Using this command, you can set the queue length of trap messages sent to the destination host. *size* specifies the queue length whose default value is 32.

----End

1.3.6 Setting the Saving Time of Trap Messages

Procedure

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

- Step 2** Run the **snmp-agent trap life** *seconds* command to set the saving time of trap messages.

Using this command, you can set the lifetime of Trap messages. When the lifetime expires, Trap messages are discarded. *seconds* is an integer and its default value is 300, in seconds.

----End

1.3.7 Checking the Configuration

Context

Run the following command to check the previous configuration.

Action	Command
Check the configuration of traps.	display current-configuration configuration include trap

1.4 Maintaining SNMP

This section describes how to maintain SNMP.

Context



CAUTION

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

When an SNMP running fault occurs, use the **debugging** command in the user view to locate the fault. For details on how to enable the debugging, refer to the chapter "Monitoring and Debugging" in the *Quidway S5300 Series Ethernet Switches Configuration Guide - Device Management*. For details of the **debugging** command, refer to the *Quidway S5300 Series Ethernet Switches Command Reference*.

Action	Command
Enable SNMP debugging.	debugging snmp-agent { header packet trap process }

1.5 Configuration Examples

This section provides several examples of SNMP.

Context

1.5.1 Example for Configuring an NMS to Manage the S-switch Through the In-Band Mode

1.5.1 Example for Configuring an NMS to Manage the S-switch Through the In-Band Mode

Context

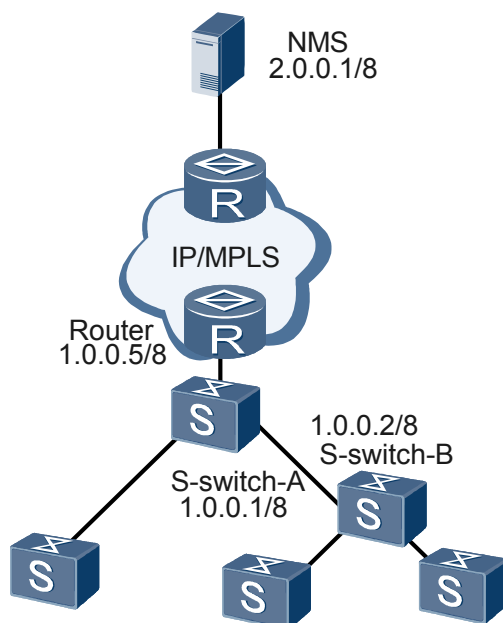
Networking Requirements

As shown in [Figure 1-3](#), the NMS is connected to the S-switch through an IP or an MPLS core network. The IP address of the NMS is 2.0.0.1 and the IP address of the router connected to S-

switch-A is 1.0.0.5. S-switch-A, which is the S3328, is connected to the router only through Eth 0/0/1. The IP address of Ethernet 0/0/1 is 1.0.0.1; the IP address of the Ethernet interface on S-switch-B is 1.0.0.2.

Networking diagram

Figure 1-3 Typical networking of configuring an NMS to manage the S-switch through the in-band mode



Configuration Procedure

1. Configure S-switch-A.

Set the IP address of S-switch-A as 1.0.0.1.

```

<Quidway> system-view
[Quidway] vlan1
[Quidway-vlan1] port ethernet 0/0/1
[Quidway-vlan1] quit
[Quidway] interface vlanif 1
[Quidway-vlanif1] ip address 1.0.0.1 8
[Quidway-vlanif1] quit

```

Set the next hop from S-switch-A to the NMS as 1.0.0.5.

```

[Quidway] ip route-static 2.0.0.1 8 1.0.0.5

```

Enable the SNMP agent and set the SNMP version to SNMPv1.

```

[Quidway] snmp-agent sys-info version v1

```

Set the community name and the access authority.

```

[Quidway] snmp-agent community read public
[Quidway] snmp-agent community write private

```

Set the contact information of the administrator, the physical location of the S-switch, and the host name.

```

[Quidway] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Quidway] snmp-agent sys-info location telephone-closet,3rd-floor
[Quidway] sysname sysadm

```

Configure the trap function.

```
[sysadm] snmp-agent trap enable
[sysadm] snmp-agent target-host trap address udp-domain 2.0.0.1 params
securityname public
```

2. Configure S-switch-B.

The configuration of S-switch-B is similar to that of S-switch-A, and is not mentioned here.

3. Configure the NMS.

Install the Huawei iManager N2000 DMS on the NMS and configure SNMP to the iManager N2000 DMS. Then, you can manage the device.

For details on configuring and using iManager N2000 DMS, refer to the *HUAWEI iManager N2000 DMS - Operator Guide*.

Configuration Files

Configuration file of S-switch-A

```
#
sysname sysadm
#
vlan batch 1
#
interface Vlanif1
ip address 1.0.0.1 255.0.0.0
#
interface Ethernet0/0/1
port default vlan 1
#
ip route-static 2.0.0.1 255.0.0.0 1.0.0.5
#
snmp-agent
snmp-agent local-engineid 000007DB7F00000100005C4B
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info contact Mr.Wang-Tel:3306
snmp-agent sys-info location telephone-closet,3rd-floor
snmp-agent sys-info version v1 v3
snmp-agent target-host trap address udp-domain 2.0.0.1 params securityname public
snmp-agent trap enable configuration
snmp-agent trap enable efm
snmp-agent trap enable flash
snmp-agent trap enable lldp
snmp-agent trap enable mstp
snmp-agent trap enable ssh
snmp-agent trap enable standard
snmp-agent trap enable system
#
return
```

The configuration file of S-switch-B is the same as that of S-switch-A except for the static route configuration and IP address of the VLANIF interface. Thus, the configuration file of S-switch-B is not mentioned here.

2 RMON Configuration

About This Chapter

This chapter describes the basics of Remote Monitoring (RMON) and the procedures for configuring RMON.

Context

[2.1 Introduction to RMON](#)

This section describes the basic principle and concept of RMON.

[2.2 Configuring the RMON Statistics Function](#)

This section describes how to view the statistics on traffic on a network through the RMON statistics function.

[2.3 Configuring the RMON Alarm Function](#)

This section describes how to configure the device to report alarms on the abnormal traffic, such as excessive broadcast packets on the local network segment, to the NMS through the RMON alarm function.

[2.4 Maintaining RMON](#)

This section describes how to maintain RMON.

[2.5 Configuration Examples](#)

This section provides several configuration examples of RMON.

2.1 Introduction to RMON

This section describes the basic principle and concept of RMON.

2.1.1 RMON

2.1.2 Implementing RMON on the S-switch

2.1.3 Logical Relationships Between Configuration Tasks

2.1.1 RMON

Applications of RMON

RMON is implemented on the basis of the Simple Network Management Protocol (SNMP) architecture, and is compatible with the existing SNMP framework. RMON consists of the Network Management Station (NMS) and the agent running on each network device.

An RMON agent collects statistics on traffic in a network, including the number of packets on a network segment in a certain period and the number of correct packets sent to a host.

RMON can monitor remote network devices more efficiently and actively. It provides an efficient solution to monitor the running of sub-networks, which reduces the communications traffic between the NMS and the agent. Large-scale networks can thus be managed in a simple and effective manner.

Methods of Collecting Information Through RMON

For RMON, more than one NMS can exist to monitor the traffic. The NMS collects management information by using the following methods:

- Through an RMON probe

An RMON probe is responsible for collecting information about network devices. The NMS thus obtains all information about the RMON Management Information Base (MIB) to control a network through the dedicated RMON probe. The NMS receives all the information of the RMON MIB through the dedicated RMON probe.

- By embedding an RMON agent into the device

The device thus can act as an RMON probe. The NMS uses basic SNMP commands to exchange data with the RMON agent and to collect management information about the network.

This method, however, has limitations. Because of limited device resources, not all data of the RMON MIB is obtained. Generally, the data of statistics, history, alarms, and events is collected.

At present, RMON supports the monitoring and statistics only on Ethernet interfaces of network devices.

2.1.2 Implementing RMON on the S-switch

The S-switch is embedded with an RMON agent module and can thus exchange RMON information with an NMS. At present, RMON implemented on the S-switch supports four

groups, namely, statistics, history, alarm, and event, defined in RFC 2819, and a Performance MIB defined by Huawei.

Statistics Group

A statistics group collects basic statistics on each monitored sub-network. The statistics collected include the volume of the traffic over a network segment, distribution of various packets, number of errored frames, and times of collisions. A statistics group only has one table named etherStatsTable.

NOTE

Compared with the output of the **display interface** command, the statistics on RMON also obtains data from the lower layer, but the statistics on RMON are more complete.

History Group

A history group collects statistics about network status periodically and stores the statistics for future use. A history group contains the historyControlTable and ethernetHistoryTable.

- The historyControlTable is used to set control information, such as the sampling intervals.
- The etherHistoryTable is used to provide a network administrator with history statistics, such as traffic over a network segment, errored packets, broadcast packets, usage, and times of collisions.

Each entry in historyControlTable can map up to 10 entries in etherHistoryTable. The previous entries in etherHistoryTable are overwritten one by one if the number of records exceeds the preset value.

Alarm Group

An alarm group presets a set of thresholds for alarm variables that can be any objects in a local MIB. The monitor records logs or sends traps to an NMS when the amount of sampled data exceeds the threshold. The alarm group contains an alarmTable.

In RFC 2819, a mechanism to delay the alarms is set down. When the sample surpasses the threshold, an event is triggered. No event will be triggered until the sample surpasses the threshold in the opposite direction. This mechanism generates an event when the sampled data surpasses the threshold in a direction, and does not generate more events until the sampled data surpasses the threshold in the opposite direction. The S-switch does not adopt this mechanism. Instead, the S-switch defines that an alarm is generated when the sampled value restores to the normal threshold.

Event Group

An event group records all the events generated by an RMON agent. When an event occurs, the event group records the event to logs or sends a trap message to the NMS. An event group contains two tables: eventTable and logTable.

An event group can output three types of events: Log, Trap, and Log-Trap. Each event entry can correspond to up to 10 logs. The previous logs are overwritten circularly if there are more logs.

Prialarm Group

Based on the alarmTable in RFC 2819, a prialarm group is enhanced with setting alarm objects in the form of expressions and the time span of an alarm entry in the form of an expression. The prialarm group contains one table, that is, prialarmTable.

Entry Capacity and TTL

In the S-switch, to save system resources, each entry is specified with a value of time to live (TTL). TTL refers to the time an entry can exist if it is in the invalid state. If the entry keeps invalid, its TTL decreases continuously. The entry is deleted, when TTL decreases to 0.

Table 2-1 shows the capacity of each table and the maximum TTL of an entry in each table.

Table 2-1 Capacity of the table and TTL

Table Name	Entry Capacity (Bytes)	Maximum TTL (Seconds)
etherStatsTable	100	600
historyControlTable	100	600
alarmTable	60	6000
eventTable	60	600
logTable	600	-
prialarmTable	50	6000

NOTE

No maximum TTL is set for the logTable. In the logTable, each event entry can correspond to up to 10 logs. The previous logs are overwritten circularly if there are more logs.

When an SIC is removed, the entries in the corresponding etherStatsTable and historyControlTable become invalid. At the same time, the value of TTL defaults to 600 seconds. If the value of TTL reaches 0, the entries are deleted.

When the SIC is installed again and the entries still exist, the entries become valid.

2.1.3 Logical Relationships Between Configuration Tasks

There is no dependence relationship between configuration tasks.

2.2 Configuring the RMON Statistics Function

This section describes how to view the statistics on traffic on a network through the RMON statistics function.

Context

2.2.3 (Optional) Configuring the etherStatsTable and **2.2.4 (Optional) Configuring the historyControlTable** are optional and not listed in sequence.

After etherStatsTable and historyControlTable are configured, you must enable the RMON statistics on the interface to obtain correct information from the tables; otherwise, all the numbers obtained from the tables are 0.

[2.2.1 Establishing the Configuration Task](#)

[2.2.2 Enabling the RMON Statistics Function on an Interface](#)

[2.2.3 \(Optional\) Configuring the etherStatsTable](#)

[2.2.4 \(Optional\) Configuring the historyControlTable](#)

[2.2.5 Checking the Configuration](#)

2.2.1 Establishing the Configuration Task

Applicable Environment

To view and monitor the statistics on traffic on a network segment, you can configure the RMON statistics function.

Pre-configuration Tasks

Before configuring the RMON statistics function, complete the following tasks:

- Configuring parameters of Ethernet interfaces
- Configuring basic SNMP functions

Data Preparation

To configure the RMON statistics function, you need the following data.

No.	Data
1	Interface on which the statistics function is enabled
2	(Optional) etherStatsTable to be used and related parameters
3	(Optional) historyControlTable to be used and related parameters

2.2.2 Enabling the RMON Statistics Function on an Interface

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 Ethernet interface view.
- Step 3** Run the **rmon-statistics enable** command to enable the RMON statistics function on the interface.

This configuration is valid for only Ethernet interfaces, including Gigabit Ethernet (GE) interfaces. If the statistics function is not enabled on an interface, the statistics in the ethernetStatsTable and the historyControlTable of RMON are 0.

----End

2.2.3 (Optional) Configuring the etherStatsTable

Context

To monitor the statistics on an interface of a device, the network administrator needs to create a table entry for the interface and specify the interface OID, entry index, and entry status. The network administrator then can read the entry to obtain the latest statistics.

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 Ethernet interface view.
- Step 3** Run the **rmon statistics entry-number [owner name** command to configure the etherStatsTable.

----End

2.2.4 (Optional) Configuring the historyControlTable

Context

The history data management function enables the device to sample a certain interface, set the maximum number of history items to be saved in the historyControlTable, set the sampling interval, collect statistics on the interface periodically, and save them to the etherHistoryTable for future use.

RMON defines that each monitored interface should provide more than two history control entries. One entry samples data every 30 seconds; the other entry samples data every 30 minutes. The sampling at shorter intervals can help probe the burst changes of traffic modes. The sampling at longer intervals can help monitor the long-term status of the interface. Currently, the device keeps up to 10 latest history control entries.

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 Ethernet interface view.
- Step 3** Run the **rmon history entry-number buckets number interval sampling-interval [owner name]** command to configure the historyControlTable.

----End

2.2.5 Checking the Configuration

Context

Run the following commands to check the previous configuration.

Action	Command
Check the RMON history.	display rmon history [ethernet <i>interface-number</i> gigabitethernet <i>interface-number</i>]
Check the RMON statistics.	display rmon statistics [ethernet <i>interface-number</i> gigabitethernet <i>interface-number</i>]

2.3 Configuring the RMON Alarm Function

This section describes how to configure the device to report alarms on the abnormal traffic, such as excessive broadcast packets on the local network segment, to the NMS through the RMON alarm function.

Context

[2.3.3 \(Optional\) Configuring the alarmTable](#) and [2.3.4 \(Optional\) Configuring the prialarmTable](#) are optional and not listed in sequence.

[2.3.1 Establishing the Configuration Task](#)

[2.3.2 Configuring the eventTable](#)

[2.3.3 \(Optional\) Configuring the alarmTable](#)

[2.3.4 \(Optional\) Configuring the prialarmTable](#)

[2.3.5 Checking the Configuration](#)

2.3.1 Establishing the Configuration Task

Applicable Environment

When the volume of traffic on a certain monitored network segment exceeds the normal value, the S-switch automatically reports alarms to an NMS. In this case, you need to configure the RMON alarm function on the S-switch.

NOTE

RMON can provide traffic statistics and report alarms, but cannot prevent any abnormalities. To remove an abnormality, you need to use other methods.

Pre-configuration Tasks

Before configuring the RMON alarm function, complete the following tasks:

- Configuring parameters of Ethernet interfaces

- Configuring basic SNMP functions

Data Preparation

To configure the RMON alarm function, you need the following data.

No.	Data
1	Interface on which the alarms function is enabled
2	(Optional) etherStatsTable to be used and related parameters
3	(Optional) eventTable to be used and related parameters
4	(Optional) alarmTable to be used and related parameters
5	(Optional) prialarmTable to be used and related parameters

2.3.2 Configuring the eventTable

Procedure

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

Step 2 Run the **rmon event entry-number [description string] { log | trap object | log-trap object | none } [owner owner-name]** command to configure the eventTable.

----End

2.3.3 (Optional) Configuring the alarmTable

Context

The RMON alarm management monitors a specified alarm variable identified by its OID at a specified sampling interval. An alarm event is generated when the monitored variable exceeds the defined threshold. Generally, the event is recorded in the log table, or RMON sends trap messages to the NMS.

If the events of *event-entry1* and *event-entry2* that correspond to the upper and lower thresholds are not configured in the eventTable, no alarm is generated even if the alarm conditions are satisfied. At this time, the alarm is in the **undercreation** state rather than the **valid** state. If either the upper or the lower threshold is created, an alarm is generated when the alarm conditions are satisfied. At this time, the alarm is in the **valid** state. If an incorrect alarm variable is created, for example, an nonexistent OID is specified, the alarm is in the **undercreation** state and no alarm is generated.

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 Ethernet interface view.
- Step 3** Run the **rmon-statistics enable** command to enable the RMON statistics function on the interface.
- Step 4** (Optional) Run the **rmon statistics entry-number [owner name** command to configure the etherStatsTable.
- Step 5** Run the **quit** command to return to the system view.
- Step 6** Run the **rmon alarm entry-number alarm-OID sampling-time { delta | absolute } rising-threshold threshold-value1 event-entry1 falling-threshold threshold-value2 event-entry2 [owner owner-name]** command to configure the alarmTable.

In **Step 6**, if the value of *alarm-oid* is set to the value of etherStatsEntry, that is, 1.3.6.1.2.1.16.1.1.1, you must perform all the preceding steps. In this case, the instance in alarm-oid must be the same as entry-number set in Step 4.

Skip **Step 4** if the value of alarm-OID is not the same as that of etherStatsEntry.

----End

2.3.4 (Optional) Configuring the prialarmTable

Context

Based on the alarmTable in RFC 2819, the RMON prialarmTable adds two functions: setting the alarm object in the form of expressions and setting the TTL of a prialarm entry.

The added entries in the prialarmTable are:

- Expressions of alarm variables. It is the arithmetic expression composed of the OIDs of alarm variables, +, -, *, /, or brackets.
- Descriptions of prialarm entries in a string of characters.
- Sampling interval variables.
- Two prialarm status types: Forever or Cycle. If Cycle is set, no alarm is generated and an entry is deleted after the specified prialarm state period.

If the events of *event-entry1* and *event-entry2* that correspond to the upper and lower thresholds are not configured in the eventTable, no alarm is generated even if the alarm conditions are satisfied. At this time, the alarm is in the **undercreation** state rather than the **valid** state. If either the upper or the lower threshold is created, an alarm is generated when the alarm conditions are satisfied. At this time, the alarm is in the **valid** state.

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 Ethernet interface view.
- Step 3** Run the **rmon-statistics enable** command to enable the RMON statistics function on the interface.

- Step 4** (Optional) Run the **rmon statistics** *entry-number* [**owner** *name*] command to configure the etherStatsTable.
- Step 5** Run the **quit** command to return to the system view.
- Step 6** Run the **rmon prialarm** *entry-number* *prialarm-formula* *description-string* *sampling-interval* { **delta** | **changeratio** | **absolute** } **rising-threshold** *threshold-value1* *event-entry1* **falling-threshold** *threshold-value2* *event-entry2* **entrytype** { **cycle** *entry-period* | **forever** } [**owner** *text-string*] command to configure the prialarmTable.

In **Step 6**, if the value of *alarm-oid* is set to the value of etherStatsEntry, that is, 1.3.6.1.2.1.16.1.1.1, you must perform all the preceding steps. In this case, the instance in alarm-oid must be the same as entry-number set in Step 4.

Skip **Step 4** if the value of alarm-OID is not the same as that of etherStatsEntry.

----End

2.3.5 Checking the Configuration

Context

Run the following commands to check the previous configuration.

Action	Command
Check the RMON alarms.	display rmon alarm [<i>entry-number</i>]
Check the RMON events.	display rmon event [<i>entry-number</i>]
Check the RMON logs.	display rmon eventlog [<i>entry-number</i>]
Check the RMON history.	display rmon history [ethernet <i>interface-number</i> gigabitethernet <i>interface-number</i>]
Check the RMON prialarmTable.	display rmon prialarm [<i>entry-number</i>]
Check the RMON statistics.	display rmon statistics [ethernet <i>interface-number</i> gigabitethernet <i>interface-number</i>]

2.4 Maintaining RMON

This section describes how to maintain RMON.

Context



CAUTION

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

When an RMON running fault occurs, run the following debugging command in the user view to locate the fault. For details on how to enable the debugging, refer to the chapter "Monitoring and Debugging" in the *Quidway S5300 Series Ethernet Switches Configuration Guide - Device Management*.

2.5 Configuration Examples

This section provides several configuration examples of RMON.

Context

2.5.1 Examples for Configuring RMON

2.5.1 Examples for Configuring RMON

Context

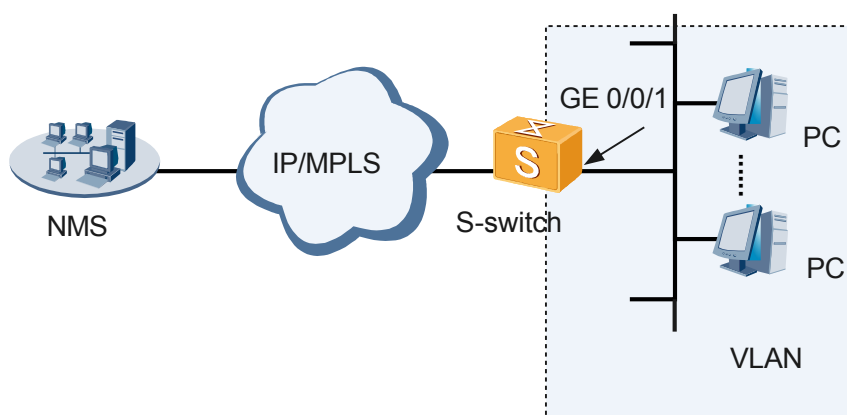
Networking Requirements

As shown in [Figure 2-1](#), Ethernet 0/0/1 on the S-switch belongs to a VLAN.

It is required that the network connected to Ethernet 0/0/1 be monitored to obtain real-time and history statistics of broadcast, multicast, and unknown unicast packets on the network.

If the number of broadcast, multicast, and unknown unicast packets in the VLAN becomes abnormal, the S-switch sends a Trap message to the NMS.

Figure 2-1 Figure 2-1 Networking diagram of configuring RMON



Configuration Roadmap

To send a Trap message to the NMS, you need to use SNMP commands to enable the Trap function and set a corresponding community name. For details, refer to the chapter [1 SNMP Configuration](#).

The configuration roadmap is as follows:

- Enable the statistics function.

- Configure the etherStatsTable.
- Configure the historyControlTable.
- Configure the eventTable.
- Configure the alarmTable.

Data Preparation

To complete the configuration, you need the following data:

- Interval for sampling data
- Threshold for triggering alarms
- Community name for communicating with the NMS

Configuration Procedure

1. Enable the statistics function.

Enable the RMON statistics function on the interface.

```
<Quidway> system-view
[Quidway] interface ethernet 0/0/1
[S-switch-ethernet0/0/1] rmon-statistics enable
```

Configure the etherStatsTable.

```
[S-switch-Ethernet0/0/1] rmon statistics 1 owner User01
```

Verify the configuration. You can check the traffic on the subnet.

```
[S-switch-Ethernet0/0/1] display rmon statistics Ethernet 0/0/1
Statistics entry 1 owned by User01 is VALID.Received :
Interface : Ethernet0/0/1<ifEntry.514>
octets      :156      , packets      :1
broadcast packets :0      , multicast packets:1
undersized packets :0      , oversized packets:0
fragments packets :0      , jabbers packets :0
CRC alignment errors:0      , collisions      :0
Dropped packet (insufficient resources):0
Packets received according to length (octets):
64      :0      , 65-127 :0      , 128-255 :1
256-511:0      , 512-1023:0      , 1024-1518:0
```

2. # Configure S-switch-A.

Sample the traffic on the subnet every 30 seconds and save the latest 10 history entries.

```
[S-switch-Ethernet0/0/1] rmon history 1 buckets 10 interval 30 owner User01
```

Verify the configuration. Only the last sampling record is displayed through CLI. To display all the history records, use the special NMS software.

```
[S-switch-Ethernet0/0/1] quit
[S-switch] display rmon history ethernet 0/0/1
History control entry 1 owned by User01 is VALID
Samples interface      : Ethernet0/0/1<ifEntry.514>
Sampling interval      : 30(sec) with 10 buckets max
Last Sampling time     : 0days 01h:56m:21s
Latest sampled values :
Dropevents            :0      , octets            :312
packets                :2      , broadcast packets :0
multicast packets      :2      , CRC alignment errors :0
undersize packets      :0      , oversize packets  :0
fragments              :0      , jabbers           :0
collisions              :0      , utilization        :0
```

3. Configure the eventTable.

Set the device to record logs for RMON event 1.

- ```
[S-switch] rmon event 1 log owner User01
```
- # Set the device to send Trap messages to the NMS for RMON event 2 and set the community name to public.
- ```
[S-switch] rmon event 2 description prialarmevent trap public owner User01
```
- # Display the alarms.
- ```
[S-switch] display rmon event
Event table 1 owned by User01 is VALID.
 Description: logevent.
 Will cause log when triggered, last triggered at 0days 00h:00m:00s.
Event table 2 owned by User01 is VALID.
 Description: prialarmevent.
 Will cause snmp-trap when triggered, last triggered at 0days 00h:00m:00s.
```
4. Configure the alarmTable for broadcast packets.
 

# Sample the broadcast packets every 30 seconds. Trigger event 1 when 10000 or more broadcast packets are received. Trigger event 2 when 100 broadcast or less broadcast packets are received.

```
[S-switch] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 30 absolute rising-threshold 10000 2 falling-threshold 100 1 owner User01
```

# Display the alarms.

```
[S-switch]display rmon alarm 1
Alarm table 1 owned by User01 is VALID.
 Samples absolute value : 1.3.6.1.2.1.16.1.1.1.6.1<etherStatsBroadcastPkts.
1>
 Sampling interval : 30(sec)
 Rising threshold : 10000(linked with event 1)
 Falling threshold : 100(linked with event 2)
 When startup enables : risingOrFallingAlarm
 Latest value : 0
```
  5. Configure the alarmTable for multicast packets.
 

# Sample the multicast packets every 30 seconds. Trigger event 1 when 50000 or more multicast packets are received. Trigger event 2 when 100 or less multicast packets are received.

```
[S-switch] rmon alarm 2 1.3.6.1.2.1.16.1.1.1.7.1 30 absolute rising-threshold 50000 2 falling-threshold 100 1 owner User01
```

# Display the alarms.

```
[S-switch] display rmon alarm 1
[S-switch] display rmon alarm 2
Alarm table 2 owned by User01 is VALID.
 Samples absolute value : 1.3.6.1.2.1.16.1.1.1.7.1<etherStatsMulticastPkts.
1>
 Sampling interval : 30(sec)
 Rising threshold : 50000(linked with event 1)
 Falling threshold : 100(linked with event 2)
 When startup enables : risingOrFallingAlarm
 Latest value : 0
```
  6. Configure the alarmTable for unknown unicast packets.
 

# Sample the unicast packets every 30 seconds. Trigger event 1 when 1000 or more unicast packets are received. Trigger event 2 when 10 or less unicast packets are received.

```
[S-switch] rmon alarm 3 1.3.6.1.2.1.2.2.1.12.898 30 absolute rising-threshold 1000 2 falling-threshold 10 1 owner User01
```

# Display the alarms.

```
[S-switch] display rmon alarm 3
Alarm table 3 owned by User01 is VALID.
 Samples absolute value : 1.3.6.1.2.1.2.2.1.12.898<ifInNUcastPkts.898>
 Sampling interval : 30(sec)
 Rising threshold : 1000(linked with event 2)
 Falling threshold : 10(linked with event 1)
```

```
When startup enables : risingOrFallingAlarm
Latest value : 0
```

## Configuration Files

```
#
sysname S-switch
#
interface Ethernet0/0/1
 rmon-statistics enable
 rmon statistics 1 owner User01
 rmon history 1 buckets 10 interval 30 owner User01
#
snmp-agent
snmp-agent local-engineid 000007DB7F000001000071B6
snmp-agent sys-info version v3
snmp-agent target-host trap address udp-domain 129.102.149.23 params securityname
public
snmp-agent trap enable system
snmp-agent trap enable standard
#
 rmon event 1 description logevent log owner User01
 rmon event 2 description prialarmeven trap public owner User01
 rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 30 absolute rising-threshold 10000 1 falling-
threshold 100 2 owner User01
 rmon alarm 2 1.3.6.1.2.1.16.1.1.1.7.1 30 absolute rising-threshold 50000 1 falling-
threshold 100 2 owner User01
 rmon alarm 3 1.3.6.1.2.1.2.2.1.12.898 30 absolute rising-threshold 1000 1 falling-
threshold 100 2 owner User01
#
return
```

# 3 HGMP Configuration

---

## About This Chapter

This chapter describes fundamental knowledge of the Huawei Group Management Protocol (HGMP) and the procedures for configuring the Neighbor Discovery Protocol (NDP), Network Topology Discovery Protocol (NTDP), and cluster.

### Context

#### [3.1 Introduction](#)

This section describes the basics of HGMP and the logical relationships between configuration tasks.

#### [3.2 Configuring NDP](#)

This section describes how to configure NDP to discover information about neighbors.

#### [3.3 Configuring NTDP](#)

This section describes how to configure NTDP to collect information about network topologies.

#### [3.4 Configuring a Cluster](#)

This section describes how to create and manage a cluster.

#### [3.5 Deleting or Quitting a Cluster](#)

This section describes how to delete or quit a cluster.

#### [3.6 Adding a Member Switch](#)

This section describes how to add a member switch on an administrator switch.

#### [3.7 Deleting a Member Switch](#)

This section describes how to delete a member switch on the administrator switch.

#### [3.8 Setting Parameters for a Cluster](#)

This section describes how to set parameters for a cluster.

#### [3.9 Maintaining HGMP](#)

This section describes how to maintain and debug a cluster.

#### [3.10 Adjusting Cluster Parameters](#)

To optimize performance parameters of the created cluster, you can adjust cluster parameters to facilitate the management and maintenance of the HGMP cluster and better manage member switches in the cluster.

### [3.11 Managing Switches in a Cluster Through HGMP](#)

### [3.12 Configuration Examples](#)

This section provides several configuration examples of a cluster.

## 3.1 Introduction

This section describes the basics of HGMP and the logical relationships between configuration tasks.

### [3.1.1 HGMP](#)

### [3.1.2 NDP](#)

### [3.1.3 NTDP](#)

### [3.1.4 Roles in a Cluster](#)

### [3.1.5 Delivery in Batches](#)

### [3.1.6 Batch Restart](#)

### [3.1.7 Incremental Configuration](#)

### [3.1.8 Synchronization of Configuration Files](#)

### [3.1.9 Security Features](#)

### [3.1.10 Plug-and-play Function](#)

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

## 3.1.1 HGMP

### Definition

HGMP is a cluster management protocol developed by Huawei.

### Function

HGMP is used to group Layer 2 devices connected to the S-switch into a unified management domain, that is, a cluster. HGMP supports automatic collection of network topologies and provides integrated maintenance and management channels. In this manner, a cluster uses only one IP address for external communications, simplifying device management and saving IP addresses.

## 3.1.2 NDP

In HGMP, NDP is used to collect information about the directly connected neighbors. The information collected includes:

- Device type
- Software version
- Hardware version
- Connected interface
- Member number

- Hardware platform

 **NOTE**

Any device that supports HGMP does not forward NDP packets.

The S-switch has an NDP table that is used to store information about neighbors.

After receiving an NDP packet from a neighbor, the S-switch compares contents of the packet with that of a corresponding entry in the NDP table and updates the entry.

### 3.1.3 NTDP

In HGMP, NTDP is used to collect information about topologies. According to neighbor information in the NDP table, the S-switch sends and forwards requests for topology information. In this manner, the S-switch collects entries in the NDP table of each device in a certain network segment.

When receiving an NTDP topology request packet, the S-switch sends an NTDP topology response packet immediately. At the same time, the S-switch forwards the received NTDP packet to other interfaces.

### 3.1.4 Roles in a Cluster

HGMP defines four roles in a cluster: administrator switch, member switch, candidate switch, and standby switch.

 **NOTE**

Currently, the S-switch cannot function as a standby switch.

- The administrator switch is the management device in the cluster. To ensure communications between a device in the cluster and a device outside the cluster, a public IP address must be assigned to the administrator switch.
- A member switch is a member device in the cluster. The member switch is managed by the administrator switch that acts as an agent. A public IP address does not need to be assigned to a member switch.
- A candidate switch is a device that has cluster functions but does not join any cluster.
- A standby switch is a backup administrator switch in the cluster. When the active administrator switch fails, the standby switch automatically becomes the administrator switch.

You can determine the role of a switch in a cluster. Each of the four different roles, however, can shift to each other in some circumstances following a certain rule.

### 3.1.5 Delivery in Batches

HGMP can perform batch distribution over all the member switches under its management. Objects to be distributed in batches include: the system software, configuration files, patch files, and license files.

- The batch distribution command can be performed only on the administrator switch.
- The administrator switch can be configured with the plug-and-play IP address, user name, and password. If no IP address, user name, or password are specified in the command, the

plug-and-play IP address, user name, and password are adopted. If neither kinds of IP address, user name, and password are configured, the command cannot be performed.

- Member switches download specified files from the FTP server and then set them as the default files for the next startup.
- To avoid congestion, you can set the maximum number of member switches that concurrently download files from the FTP server.

### 3.1.6 Batch Restart

HGMP can perform batch restart over a specified group of member switches.

- During the process of batch restart, member switches do not save the current configuration.
- After receiving the batch restart command, member switches wait 1 second to guarantee the pervasion of control packets throughout the cluster.

### 3.1.7 Incremental Configuration

In a cluster, some member switches may have the same configurations, such as creating a VLAN and enabling a feature. The incremental configuration function is used to remotely control the selected member switches in batches. With this mode, you only need to configure a control command list on the administrator switch. Then, you can deliver the control command list to member switches at a time and query the control command output on each member switch. The member selection mode can be all, device type-based, member switch ID-based, or IP address-based.

- Incremental configuration can be performed only on the administrator switch.
- Incremental configuration is applied to the scenario of configuring member switches in batches and is performed once on selected switches.
- After incremental configuration is performed, a result list is returned to report the command output on each member switch. If an error occurs during the command execution, the faulty command can be located according to the sequence number.
- Latter execution results of the incremental configuration overwrite previous ones and only the last result is saved.
- You can edit a configuration command list in the incremental configuration view. The command execution is closely related to specific views and its sequence is the same as that on a device.

### 3.1.8 Synchronization of Configuration Files

After a cluster is created and configured with basic functions, you can save the configuration files of the cluster members to a specified FTP server through the configuration synchronization command.

- To perform configuration synchronization, you need to specify an FTP server in advance.

### 3.1.9 Security Features

After a cluster is created and configured with basic functions, you can close the network edge of the cluster as required and then the topology of the cluster becomes stable. When plug and play is enabled, a great number of Layer 2 interfaces are automatically enabled with NDP and NTDP on member switches. NDP and NTDP, however, are not required on interfaces unrelated to the cluster. Therefore, you need to disable NDP or NTDP on unrelated interfaces. As a result, less packets are transmitted and the topology of the cluster is stable.

- On the administrator switch, disable NDP or NTDP on unrelated interfaces in the cluster.
- After you disable NDP on unrelated interfaces in the cluster, NDP packets of the interfaces are not sent to the administrator switch.
- After you disable NTDP on unrelated interfaces in the cluster, NTDP packets of the interfaces are not sent to the administrator switch.
- When the topology of the cluster becomes stable, the unrelated interfaces in the cluster are defined as interfaces that have not NDP neighbors.

### 3.1.10 Plug-and-play Function

Before a device joins a cluster, you need to configure the device manually. When a great number of devices need to be added to a cluster, you can use plug and play to simplify the process. You can control the performance of basic configuration on devices. Then, connect devices to the cluster devices physically. After that, the devices can be added to the cluster automatically.

- Plug and play needs to be enabled on the administrator switch.
- The interfaces connecting the administrator switch and the member switches need to be added to a control VLAN in trunk mode.
- The interval for collecting NTDP packets needs to be set on the administrator switch.

### 3.1.11 Logical Relationships Between Configuration Tasks

- Plan the network and define the range of a cluster.
- Configure NDP and NTDP according to the network plan. For details on how to configure NDP and NTDP, see sections "[3.2 Configuring NDP](#)" and "[3.3 Configuring NTDP](#)."
- Select one switch as the administrator switch for setting up a cluster. For details on how to set up a cluster, see section "[3.4 Configuring a Cluster](#)."
- Add other switches included in the network plan into the cluster. For details on how to add switches into a cluster, see section "[3.5.4 Checking the Configuration](#)."
- Manage a cluster. For details on how to manage a cluster, see section "[3.8 Setting Parameters for a Cluster](#)."



#### NOTE

By default, HGMP is enabled on the S-switch.

## 3.2 Configuring NDP

This section describes how to configure NDP to discover information about neighbors.

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

### [3.2.2 Enabling NDP](#)

### [3.2.3 \(Optional\) Configuring the Holding Time of NDP Packets](#)

### [3.2.4 \(Optional\) Setting the Interval for Sending NDP Packets](#)

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

## 3.2.1 Establishing the Configuration Task

### Applicable Environment

When you need to set up or manage a cluster, you can use NDP to discover information about neighbors. In this case, you can configure NDP.

### Pre-configuration Tasks

None.

### Data Preparation

To configure NDP, you need the following data.

| No. | Data                                        |
|-----|---------------------------------------------|
| 1   | (Optional) Aging time of NDP packets        |
| 2   | (Optional) Interval for sending NDP packets |

## 3.2.2 Enabling NDP

### Context

To enable an interface to receive and send NDP packets, you must perform the following steps:

- Enabling NDP in the system view
- Enabling NDP on an interface
- Configuring an interface to allow NDP packets to pass through

The preceding steps are not listed in sequence.

### Enabling the System NDP

1. Run the **system-view** command to enter the system view.
2. Run the **ndp enable** command to enable the system NDP.

By default, the system NDP is enabled.

### Enabling NDP on an Interface

1. Run the **system-view** command to enter the system view.
2. Run the following command as required:
  - Run the **ndp enable** command to enable NDP on an interface in the system view.
  - Run the **interface interface-type interface-number** command to enter the interface view, and then run the **ndp enable** command to enable NDP on the interface.

By default, NDP is enabled on an interface.

## Configuring an Interface to Allow NDP Packets to Pass Through

1. Run the **system-view** command to enter the system view.
2. Run the **interface** *interface-type interface-number* command to enter the interface view.
3. Run the **bpdu enable** command to allow NDP packets to pass through the interface.

By default, NDP packet is allowed to pass through an interface.

Using the **bpdu enable** command, you can enable an interface to allow the following types of packets to pass through:

- NDP packets
- NTDP packets
- Bridge protocol data units (BPDUs) defined by the 802.3ah protocol
- BPDUs defined by the Link Layer Discovery Protocol (LLDP)
- BPDUs defined by the Spanning Tree Protocol (STP)
- BPDUs defined by the Rapid Spanning Tree Protocol (RSTP)
- BPDUs defined by the Multiple Spanning Tree Protocol (MSTP)

For details about the **bpdu enable** command, refer to the *Quidway S5300 Series Ethernet Switches Configuration Guide - Ethernet* and the *Quidway S5300 Series Ethernet Switches Command Reference*.

### 3.2.3 (Optional) Configuring the Holding Time of NDP Packets

#### Context

By default, the aging time of NDP packets is set to 180 seconds. The aging time of NDP packets must be longer than the interval for sending NDP packets.

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ndp timer aging** *aging-time* command to set the aging time of NDP packets.
- End

### 3.2.4 (Optional) Setting the Interval for Sending NDP Packets

#### Context

By default, the interval for sending NDP packets is set to 60 seconds. The interval for sending NDP packets must be shorter than the aging time of NDP packets.

#### Procedure

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

**Step 2** Run the **ndp timer hello interval** command to set the interval for sending NDP packets.

----End

## 3.2.5 Checking the Configuration

### Context

Run the following commands in the user view to check the previous configuration.

| Action                                                                          | Command                                                                                                |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Check the NDP settings.                                                         | <b>display ndp</b>                                                                                     |
| Check the neighbor information discovered by a specified interface through NDP. | <b>display ndp interface</b> { <i>interface-type interface-number</i> [ <i>to interface-number</i> ] } |

Run the preceding commands, and you can obtain the following information:

```
<Quidway> display ndp interface gigabitethernet 0/0/14
Interface: GigabitEthernet0/0/14
 Status: Enabled, Pkts Snd: 594, Pkts Rvd: 587, Pkts Err: 0
 Neighbor 1: Aging Time: 85(s)
 MAC Address : 0000-8600-0037
 Port Name : GigabitEthernet0/0/23
 Software Ver: Version 5.30 (V100R002C02B050)
 Device Name : Quidway
 Port Duplex : NULL
 Product Ver : S5326TP-EI
```

- The system NDP is enabled and NDP is also enabled on the specified interface.
- NDP parameters are properly set.
- Neighbors can be discovered.

## 3.3 Configuring NTDP

This section describes how to configure NTDP to collect information about network topologies.

### Context

If you skip [3.3.5 \(Optional\) Configuring the Interval for Collecting Topology Information](#), you must manually perform [3.3.6 \(Optional\) Enabling Topology Information Collection](#) to collect information about network topologies. Therefore, it is recommended that you perform [3.3.5 \(Optional\) Configuring the Interval for Collecting Topology Information](#).

[3.3.1 Establishing the Configuration Task](#)

[3.3.2 Enabling NTDP](#)

[3.3.3 \(Optional\) Configuring the Topology Collection Range](#)

[3.3.4 \(Optional\) Configuring the Delay for Forwarding NTDP Packets](#)

[3.3.5 \(Optional\) Configuring the Interval for Collecting Topology Information](#)[3.3.6 \(Optional\) Enabling Topology Information Collection](#)[3.3.7 Checking the Configuration](#)

## 3.3.1 Establishing the Configuration Task

### Applicable Environment

When you need to set up or manage a cluster, you can collect information about network topologies by using NTDP. In this case, you need to configure NTDP.

### Pre-configuration Tasks

None.

### Data Preparation

To configure NTDP, you need the following data.

| No. | Data                                                                                          |
|-----|-----------------------------------------------------------------------------------------------|
| 1   | (Optional) Segment of the network for which the topology is collected                         |
| 2   | (Optional) Delay of hops and on an interface when NTDP topology request packets are forwarded |
| 3   | (Optional) Interval for collecting topology information                                       |

## 3.3.2 Enabling NTDP

### Context

To enable an interface to receive and send NTDP packets, you must perform the following steps:

- Enabling the system NTDP
- Enabling NTDP on an interface
- Configuring an interface to allow NTDP packets to pass through

The preceding steps are not listed in sequence.

### Enabling the System NTDP

1. Run the **system-view** command to enter the system view.
2. Run the **ntdp enable** command to enable the system NTDP.

By default, the system NTDP is enabled.

## Enabling NTDP on an Interface

1. Run the **system-view** command to enter the system view.
2. Run the **interface** *interface-type interface-number* command to enter the interface view.
3. Run the **ntdp enable** command to enable NTDP on the interface.

By default, NTDP is enabled on an interface.

## Configuring an Interface to Allow NTDP Packets to Pass Through

1. Run the **system-view** command to enter the system view.
2. Run the **interface** *interface-type interface-number* command to enter the interface view.
3. Run the **bpdu enable** command to set the interface to allow NTDP packets to pass through.

By default, NTDP packet is allowed to pass through an interface.

### 3.3.3 (Optional) Configuring the Topology Collection Range

#### Context

By default, the topology collection range is 3 hops. The greater the value is, the more the memory is occupied.

#### Procedure

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

**Step 2** Run the **ntdp hop** *hop-value* command to configure the topology collection range.

----End

### 3.3.4 (Optional) Configuring the Delay for Forwarding NTDP Packets

#### Context

#### Configuring the Hop Delay for Forwarding NTDP Packets

1. Run the **system-view** command to enter the system view.
2. Run the **ntdp timer hop-delay** *time* command to set the hop delay for forwarding NTDP packets.

By default, the hop delay for forwarding NTDP packets is set to 200 ms.

#### Configuring the Interface Delay for Forwarding NTDP Packets

1. Run the **system-view** command to enter the system view.
2. Run the **ntdp timer port-delay** *time* command to set the interface delay for forwarding NTDP packets.

By default, the interface delay for forwarding NTDP packets is set to 20 ms.

### 3.3.5 (Optional) Configuring the Interval for Collecting Topology Information

#### Context

By default, the interval for collecting topology information is set to 0 minutes, that is, no topology information is regularly collected.

#### Procedure

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

**Step 2** Run the **ntdp timer interval** command to set the interval for collecting topology information.

----End

### 3.3.6 (Optional) Enabling Topology Information Collection

#### Context

You can run the **ntdp explore** command to collect topology information at any time.

Do as follows in the user view.

#### Procedure

Run the **ntdp explore** command to enable topology information collection.

----End

### 3.3.7 Checking the Configuration

#### Context

Run the following commands in the user view to check the previous configuration.

| Action                                      | Command                                     |
|---------------------------------------------|---------------------------------------------|
| Check the global NTDP information.          | <b>display ntdp</b>                         |
| Check device information collected by NTDP. | <b>display ntdp device-list [ verbose ]</b> |

If the configuration succeeds, you can obtain the following information after running the preceding commands:

```
<HUAWEI_0.Quidway> display ntdp device-list verbose
 Hostname : HUAWEI_0.Quidway
 MAC : 0018-1111-2323
 Hop : 0
```

```

Platform : S5300
IP : 172.19.250.1/24
Version : Version 5.30 (V100R002C02B050)
Cluster : Administrator switch of cluster HUAWEI

Peer MAC Native Port ID Peer Port ID N-Index P-Index Speed Dup
0000-8600-0037 GigabitEthernet0/0/14 GigabitEthernet0/0/23 2050 3202
100 NULL

Hostname : HUAWEI_1.Quidway
MAC : 0000-8600-0037
Hop : 1
Platform : S5300
IP : 172.19.250.2/24
Version : Version 5.30 (V100R002C02B050)
Cluster : Member switch of cluster HUAWEI , Administrator MAC: 0018-1111-2323

Peer MAC Native Port ID Peer Port ID N-Index P-Index Speed Dup
0018-1111-2323 GigabitEthernet0/0/23 GigabitEthernet0/0/14 3202 2050
100 NULL

```

- NTDP is enabled.
- NTDP parameters are properly set.
- Network topologies can be collected.

## 3.4 Configuring a Cluster

This section describes how to create and manage a cluster.

### Context

[3.4.1 Establishing the Configuration Task](#)

[3.4.2 Configuring a Management VLAN](#)

[3.4.3 Enabling the Cluster Function](#)

[3.4.4 Creating a Cluster](#)

[3.4.5 Checking the Configuration](#)

### 3.4.1 Establishing the Configuration Task

#### Applicable Environment

If you want to manage devices in an administrative domain through a cluster, you must configure the cluster first.

#### Pre-configuration Tasks

Before performing other configurations, you must enable the cluster function. It is recommended that you configure NDP and NTDP first to enable the administrator switch to find network topologies and candidate switches.

## Data Preparation

To configure a cluster, you need the following data.

| No. | Data                                                                                                                    |
|-----|-------------------------------------------------------------------------------------------------------------------------|
| 1   | Range of private IP addresses used in the cluster                                                                       |
| 2   | (Optional) Management virtual LAN (VLAN) ID                                                                             |
| 3   | Cluster name                                                                                                            |
| 4   | (Optional) Holdtime for the administrator switch waiting handshake packets from members                                 |
| 5   | (Optional) Interval for regularly sending handshake packets                                                             |
| 6   | (Optional) IP address of a network management system (NMS) host                                                         |
| 7   | (Optional) IP addresses of the File Transfer Protocol (FTP) server and the Trivial File Transfer Protocol (TFTP) server |
| 8   | (Optional) IP address of the log host                                                                                   |

### 3.4.2 Configuring a Management VLAN

#### Context



#### CAUTION

After a VLAN is configured as a management VLAN, it is recommended that you enable only HGMP in the management VLAN. Avoid other services, such as the Rapid Ring Protection Protocol (RRPP) and multicast services in the same VLAN.

On an administrator switch, if the ID of a management VLAN is changed or the management VLAN and its corresponding VLANIF interface are deleted, the cluster is automatically deleted.

On a member switch, if the ID of a management VLAN is changed or the management VLAN and its corresponding VLANIF interface are deleted, the member switch automatically quits the cluster.

#### Procedure

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

**Step 2** Run the **vlan *vlan-id*** command to create a VLAN and enter the VLAN view.

By default, the management VLAN of the S-switch is VLAN 1, which must be created manually.

- If you do not need to change the default management VLAN, you can skip step 6 and step 7. Here, the value of **vlan-id** in step 2 is **1**.

- If you need to change the ID of the management VLAN, values of **vlan-id** in step 2, step 4, and step 7 must be the same.

**Step 3** Run the **quit** command to quit the VLAN view.

**Step 4** Run the **interface vlanif** *vlan-id* command to create a VLANIF interface and enter the VLANIF view.

**Step 5** Run the **quit** command to quit the VLANIF view.

**Step 6** Run the **cluster** command to enter the cluster view.

**Step 7** Run the **mngvlanid** *vlan-id* command to configure a management VLAN for the cluster.

----End

### 3.4.3 Enabling the Cluster Function

#### Context

By default, the cluster function is disabled on the S-switch.

#### Procedure

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

**Step 2** Run the **cluster enable** command to enable the cluster function.

----End

### 3.4.4 Creating a Cluster

#### Context

The S-switch supports two ways to create a cluster:

- **Creating a Cluster Manually**  
In this mode, you need to manually add member switches.
- **Creating a Cluster Automatically**  
In this mode, the administrator switch prompts you whether to add all candidate switches that are found to a cluster.

#### Creating a Cluster Manually

1. Run the **system-view** command to enter the system view.
2. Run the **cluster** command to enter the cluster view.
3. Run the **ip-pool administrator-ip-address { mask-length | mask }** command to set the range of private IP addresses used in the cluster.  
Perform this step only when a cluster is not set up. If the cluster is set up, you are not allowed to change the range of private IP addresses used in the cluster.
4. Run the **build cluster-name** command to set the names of the administrator switch and the cluster, and then create a cluster.

Perform this step only on an administrator switch, or on a switch that does not belong to any cluster.

## Creating a Cluster Automatically

1. Run the **system-view** command to enter the system view.
2. Run the **cluster** command to enter the cluster view.
3. Run the **ip-pool administrator-ip-address { mask-length | mask }** command to set the range of private IP addresses used in the cluster.

Perform this step only when a cluster is not set up. If the cluster is set up, you are not allowed to change the range of private IP addresses used in the cluster.

4. Run the **auto-build [ recover ]** command to create a cluster automatically.

Perform this step only on an administrator switch, or on a switch that does not belong to any cluster. The **auto-build** command can also be used to add member switches automatically. For details, see section "[3.6 Adding a Member Switch](#)."

## System Prompts

The following error messages may be displayed when a cluster is created.

- If the following message is displayed,  
Info:Vlanif of management vlan ID does not exist, please configure.  
it indicates that no VLANIF interface is created before you create a cluster.
- If the following message is displayed,  
Info:Please specify ip-pool first.  
it indicates that the range of private IP addresses used in the cluster is not set before you create a cluster.

## 3.4.5 Checking the Configuration

### Context

Run the following commands in the user view to check the previous configuration.

| Action                                        | Command                                                                 |
|-----------------------------------------------|-------------------------------------------------------------------------|
| Check the status and statistics of a cluster. | <b>display cluster</b>                                                  |
| Check information about candidate switches.   | <b>display cluster candidates [ mac-address mac-address   verbose ]</b> |
| Check information about member switches.      | <b>display cluster members [ member-number   verbose ]</b>              |

#### NOTE

The **display cluster candidates [ mac-address mac-address | verbose ]** command and the **display cluster members [ member-number | verbose ]** command can be performed only on the administrator switch.

If the configuration succeeds, you can obtain the following information after running the preceding commands:

```
[HUAWEI_0.Quidway] display cluster
Cluster name:"HUAWEI"
Role:Administrator switch

management vlan id : 1(default vlan)
Cluster multicast MAC address : 0180-c200-000a(default)
Cluster auto-join : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP pool:172.19.250.1/24
No logging host configured
No SNMP host configured
No FTP server configured
No TFTP server configured
No SFTP server configured
cluster-member ftp-timeout: 1200 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
There are 2 member(s) in the cluster, and 0 of them are down.
[HUAWEI_0.Quidway] display cluster members
The list of cluster member:
```

| SN | Device Type | MAC Address    | Status | Device Name      |
|----|-------------|----------------|--------|------------------|
| 0  | S5300       | 0018-1111-2323 | Admin  | HUAWEI_0.Quidway |
| 1  | S5300       | 0000-8600-0037 | Up     | HUAWEI_1.Quidway |

- The cluster is created and parameters are set properly.
- Candidate switches can be discovered.
- Member switches are added to the cluster.

## 3.5 Deleting or Quitting a Cluster

This section describes how to delete or quit a cluster.

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

### [3.5.2 Deleting a Cluster](#)

### [3.5.3 Quitting a Cluster](#)

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

## 3.5.1 Establishing the Configuration Task

### Applicable Environment

If you do not need to manage switches in a domain, which is configured as a cluster, you can delete or quit the cluster.

### Pre-configuration Tasks

Before performing other configurations, you must make sure that the cluster is created. The device to quit is under the management of the cluster.

## Data Preparation

None.

### 3.5.2 Deleting a Cluster

#### Context

Do as follows on an administrator switch to delete a cluster.

#### Procedure

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

**Step 2** Run the **undo cluster enable** command to delete a cluster.

----End

### 3.5.3 Quitting a Cluster

#### Context

Do as follows on a member switch to quit a cluster.

#### Procedure

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

**Step 2** Run the **undo cluster enable** command to quit a cluster.

----End

### 3.5.4 Checking the Configuration

#### Context

Run the following commands in user view to check the previous configuration.

| Action                                        | Command                                                                  |
|-----------------------------------------------|--------------------------------------------------------------------------|
| Check the status and statistics of a cluster. | <b>display cluster</b>                                                   |
| Check information about member switches.      | <b>display cluster members</b> [ <i>member-number</i>   <b>verbose</b> ] |

Run the **display cluster** command on the administrator switch, and the following message is displayed:

Info: Cluster is not enabled.

This message indicates that the cluster is deleted.

Run the **display cluster members** [ *member-number* | **verbose** ] command on the administrator switch. If the cluster displayed does not include the deleted member switch, it indicates that the member switch quits the cluster.

Run the **display cluster** command on the member switch, and the following message is displayed:

```
Info: Cluster is not enabled.
```

This message indicates that the member switch quits the cluster.

## 3.6 Adding a Member Switch

This section describes how to add a member switch on an administrator switch.

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

### [3.6.2 Adding a Member Switch](#)

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

## 3.6.1 Establishing the Configuration Task

### Applicable Environment

If you need to manage a switch in a cluster but the switch is not a member switch, you can add it to the cluster.

### Pre-configuration Tasks

Before adding a member switch, you must enable the cluster function on the candidate switches.

### Data Preparation

To add a member switch, you need the following data.

| No. | Data                                |
|-----|-------------------------------------|
| 1   | Member IDs of candidate switches    |
| 2   | MAC addresses of candidate switches |

## 3.6.2 Adding a Member Switch

### Context

After a cluster is set up, you can add member switches to the cluster either manually or automatically.

### Adding a Member Switch Manually

In this mode, you must manually specify the MAC address of a specified member switch.

Do as follows only on the administrator switch.

1. Run the **system-view** command to enter the system view.
2. Run the **cluster** command to enter the cluster view.
3. Run the **add-member** [ *member-number* ] **mac-address** *mac-address* [ **password** *password* ] command to add a member switch.

## Adding a Member Switch Automatically

In this mode, the administrator switch prompts you whether to add the existing candidate switches to a cluster. If the authentication mode is set, the administrator switch turns down the action of adding a member switch.

Do as follows only on the administrator switch.

1. Run the **system-view** command to enter the system view.
2. Run the **cluster** command to enter the cluster view.
3. Run the **auto-build** command to automatically add a member switch.

The **auto-build** command can also be used to create a cluster automatically. For details, see section "[3.4.4 Creating a Cluster](#)."

## 3.6.3 Checking the Configuration

### Context

Run the following commands to check the previous configuration.

| Action                                        | Command                                                                  |
|-----------------------------------------------|--------------------------------------------------------------------------|
| Check the status and statistics of a cluster. | <b>display cluster</b>                                                   |
| Check information about member switches.      | <b>display cluster members</b> [ <i>member-number</i>   <b>verbose</b> ] |

If the configuration succeeds, you can obtain the following information after running the preceding commands:

The status of member switchs getting file:

| SN | Device | MacAddress     | IPAddress | Result         |
|----|--------|----------------|-----------|----------------|
| 2  | S5300  | 0003-0003-0003 | 10.0.0.3  | <b>Succeed</b> |
| 3  | S5300  | 0004-0004-0004 | 10.0.0.4  | <b>Succeed</b> |

Member switches are added to the cluster.

## 3.7 Deleting a Member Switch

This section describes how to delete a member switch on the administrator switch.

### 3.7.1 Establishing the Configuration Task

[3.7.2 Deleting a Member Switch](#)

[3.7.3 Checking the Configuration](#)

## 3.7.1 Establishing the Configuration Task

### Applicable Environment

If you do not need to manage a switch in a management domain, you can delete the switch from the cluster.

### Pre-configuration Tasks

Before deleting a member switch, make sure that the member switch to be deleted belongs to the cluster.

### Data Preparation

To delete a member switch, you need the following data.

| No. | Data                        |
|-----|-----------------------------|
| 1   | Number of the member switch |

## 3.7.2 Deleting a Member Switch

### Context

Do as follows only on the administrator switch.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **cluster** command to enter the cluster view.
- Step 3** Run the **delete-member** *member-number* command to delete a member switch.
- End

## 3.7.3 Checking the Configuration

### Context

Run the following commands in the user view to check the previous configuration.

| Action                                        | Command                |
|-----------------------------------------------|------------------------|
| Check the status and statistics of a cluster. | <b>display cluster</b> |

| Action                                   | Command                                                                  |
|------------------------------------------|--------------------------------------------------------------------------|
| Check information about member switches. | <b>display cluster members</b> [ <i>member-number</i>   <b>verbose</b> ] |

If the configuration succeeds, you can obtain the following information after running the preceding commands:

The deleted member switch is not included in the cluster.

## 3.8 Setting Parameters for a Cluster

This section describes how to set parameters for a cluster.

[3.8.1 Configuring the Interval for Sending Handshake Packets](#)

[3.8.2 Configuring the Holdtime of Handshake Packets](#)

[3.8.3 Enabling Candidate Switches to Join a Cluster Automatically](#)

[3.8.4 Setting the Aging Time of Member Switches](#)

[3.8.5 Configuring a Multicast Address for a Cluster](#)

[3.8.6 Configuring the Mode for Interfaces in the Cluster to Join a VLAN](#)

[3.8.7 Configuring the Pubic Server and Host](#)

### 3.8.1 Configuring the Interval for Sending Handshake Packets

#### Context

By default, the interval for sending handshake packets is 10 seconds. This interval must be equal to or less than one third of the holdtime of handshake packets.

Do as follows only on the administrator switch.

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
  - Step 2** Run the **cluster** command to enter the cluster view.
  - Step 3** Run the **timer interval** command to set the interval for sending handshake packets.
- End

### 3.8.2 Configuring the Holdtime of Handshake Packets

#### Context

By default, the holdtime of handshake packets is set to 60 seconds. The holdtime must be at least three times the interval for sending handshake packets.

Do as follows only on the administrator switch.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
  - Step 2** Run the **cluster** command to enter the cluster view.
  - Step 3** Run the **holdtime** *hold-time* command to set the holdtime of handshake packets on the S-switch.
- End

### 3.8.3 Enabling Candidate Switches to Join a Cluster Automatically

#### Context

Do as follows only on the administrator switch.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
  - Step 2** Run the **cluster** command to enter the cluster view.
  - Step 3** Run the **cluster-autojoin** command to enable candidate switches to join the cluster automatically.
- End

### 3.8.4 Setting the Aging Time of Member Switches

#### Context

By default, the aging time is 0 hours, that is, no aging is performed.

Do as follows only on the administrator switch.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
  - Step 2** Run the **cluster** command to enter the cluster view.
  - Step 3** Run the **cluster-discagingtime** *disconnect-aging-time* command to set the aging time of member switches.
- End

### 3.8.5 Configuring a Multicast Address for a Cluster

#### Context

Do as follows only on the administrator switch.

## Procedure

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

**Step 2** Run the **cluster** command to enter the cluster view.

**Step 3** Run the **cluster-multimac mac-address** command to set a multicast address for the cluster.

By default, the multicast address of a cluster is 01-80-C2-00-00-0A. For details on the range of multicast addresses, refer to the *Quidway S5300 Series Ethernet Switches Command Reference*.

----End

## 3.8.6 Configuring the Mode for Interfaces in the Cluster to Join a VLAN

### Context

Do as follows only on the administrator switch.

### Procedure

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

**Step 2** Run the **cluster** command to enter the cluster view.

**Step 3** Run the **port-tagged vlan** command to add interfaces in the cluster to the management VLAN in trunk mode.

----End

## 3.8.7 Configuring the Pubic Server and Host

### Context

Do as follows only on the administrator switch.

### Procedure

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

**Step 2** Run the **cluster** command to enter the cluster view.

**Step 3** (Optional) Run the **ftp-server ip-address** command to set a public FTP server for the cluster.

**Step 4** (Optional) Run the **tftp-server ip-address** command to set a public TFTP server for the cluster.

**Step 5** (Optional) Run the **snmp-host ip-address** command to set the public SNMP host for the cluster.

**Step 6** (Optional) Run the **logging-host ip-address** command to set the public log host for the cluster.

By accessing the administrator switch, member switches can access servers and hosts that are configured through [Step 3](#) to [Step 6](#).

Steps from [Step 3](#) to [Step 6](#) are not listed in sequence.

By default, no public server or host is set for a cluster.

----End

## 3.9 Maintaining HGMP

This section describes how to maintain and debug a cluster.

### Context

[3.9.1 Clearing the Statistics of NDP](#)

[3.9.2 Debugging NDP](#)

[3.9.3 Debugging NTDP](#)

[3.9.4 Debugging a Cluster](#)

### 3.9.1 Clearing the Statistics of NDP

#### Context



#### CAUTION

NDP statistics cannot be restored after you clear it. Therefore, confirm the action before you use the command.

---

To clear the statistics of NDP, run the following command in the user view.

| Action                       | Command                                                                                                                                  |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Clear the statistics of NDP. | <b>reset ndp statistics</b> [ <b>interface</b> { <i>interface-type</i> <i>interface-number</i> [ <b>to</b> <i>interface-number</i> ] } ] |

### 3.9.2 Debugging NDP

#### Context



#### CAUTION

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

---

When an NDP fault occurs, run the **debugging** command in the user view to locate the fault.

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

| Action                | Command                                                                                                                                  |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Enable NDP debugging. | <b>debugging ndp packet</b> [ <b>interface</b> { <i>interface-type</i> <i>interface-number</i> [ <b>to</b> <i>interface-number</i> ] } ] |

### 3.9.3 Debugging NTDP

#### Context

When an NTDP fault occurs, run the **debugging** command in the user view to debug NTDP, view information about debugging, locate the fault, and then analyze the cause.

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

| Action                 | Command                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------|
| Enable NTDP debugging. | <b>debugging ntdp</b> { <b>all</b>   <b>data</b>   <b>error</b>   <b>message</b>   <b>packet</b> } |

### 3.9.4 Debugging a Cluster

#### Context

When a fault occurs on a cluster, run the following **debugging** command in the user view to debug the cluster, view debugging information, locate the fault, and then analyze the cause.

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

| Action                    | Command                                                                                                                                            |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable cluster debugging. | <b>debugging cluster</b> { <b>all</b>   <b>event</b>   <b>handshake</b>   <b>member</b>   <b>mrc</b>   <b>nat</b>   <b>packet</b>   <b>state</b> } |

## 3.10 Adjusting Cluster Parameters

To optimize performance parameters of the created cluster, you can adjust cluster parameters to facilitate the management and maintenance of the HGMP cluster and better manage member switches in the cluster.

#### 3.10.1 Establishing the Configuration Task

### [3.10.2 Configuring the Interval for Sending Handshake Packets](#)

### [3.10.3 Configuring the Holdtime of Packets](#)

Configuring the Holdtime of Packets

### [3.10.4 Enabling Candidate Switches to Join a Cluster Automatically](#)

### [3.10.5 Setting the Aging Time of Member Switches](#)

Setting the Aging Time of Member Switches

### [3.10.6 Configuring a Multicast Address for a Cluster](#)

Configuring a Multicast Address for a Cluster

### [3.10.7 Configuring the Mode for Interfaces in the Cluster to Join a VLAN](#)

Configuring the Mode for Interfaces in the Cluster to Join a VLAN

### [3.10.8 Configuring Public Servers and Hosts for a Cluster](#)

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

## 3.10.1 Establishing the Configuration Task

### Applicable Environment

To optimize performance parameters of the created cluster, you can adjust cluster parameters to facilitate the management and maintenance of the HGMP cluster and better manage member switches in the cluster.

### Pre-configuration Tasks

A cluster is created by following the steps described in [3.4 Configuring a Cluster](#) and [3.8 Setting Parameters for a Cluster](#).

### Data Preparation

To configure NDP, you need the following data.

| No. | Data                                                                                                                           |
|-----|--------------------------------------------------------------------------------------------------------------------------------|
| 1   | Interval for sending handshake packets                                                                                         |
| 2   | Holdtime of packets                                                                                                            |
| 3   | Aging time of member switches                                                                                                  |
| 4   | Multicast address of the cluster                                                                                               |
| 5   | IP addresses of the public FTP server, TFTP server, SFTP server, log host, SNMP host used in the cluster                       |
| 6   | Default information about the FTP server that is configured for the cluster, including the IP address, user name, and password |

## 3.10.2 Configuring the Interval for Sending Handshake Packets

### Context

Do as follows on the administrator switch.

### Procedure

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

**Step 2** Run the **cluster** command to enter the cluster view.

**Step 3** Run the **timer interval** command to set the interval for sending handshake packets.

By default, the interval for sending handshake packets is 10 seconds. This interval must be equal to or less than one third of the holdtime of packets.

----End

## 3.10.3 Configuring the Holdtime of Packets

Configuring the Holdtime of Packets

Do as follows on the administrator switch.

### Procedure

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

**Step 2** Run the **cluster** command to enter the cluster view.

**Step 3** Run the **holdtime hold-time** command to set the holdtime of packets.

By default, the holdtime of packets is 60 seconds. The holdtime of packets must be greater than or equal to three times the interval for sending handshake packets.

----End

## 3.10.4 Enabling Candidate Switches to Join a Cluster Automatically

Do as follows on the administrator switch.

### Procedure

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

**Step 2** Run the **cluster** command to enter the cluster view.

**Step 3** Run the **cluster-autojoin** command to enable candidate switches to join the cluster automatically.

----End

### 3.10.5 Setting the Aging Time of Member Switches

Setting the Aging Time of Member Switches

Do as follows on the administrator switch.

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **cluster** command to enter the cluster view.
- Step 3** Run the **cluster-discagingtime** *disconnect-aging-time* command to set the aging time of member switches.

By default, no aging time is set, which indicates that no aging is performed.

----End

### 3.10.6 Configuring a Multicast Address for a Cluster

Configuring a Multicast Address for a Cluster

Do as follows on the administrator switch.

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **cluster** command to enter the cluster view.
- Step 3** Run the **cluster-multimac** *mac-address* command to configure a multicast address for a cluster.

By default, the multicast address of the cluster is 0180-C200-000A. Multicast addresses range from 0180-C200-0001 to 0180-C200-0007, from 0180-C200-0009 to 0180-C200-0010, and from 0180-C200-0020 to 0180-C200-002F.

----End

### 3.10.7 Configuring the Mode for Interfaces in the Cluster to Join a VLAN

Configuring the Mode for Interfaces in the Cluster to Join a VLAN

Do as follows on the administrator switch.

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **cluster** command to enter the cluster view.

**Step 3** Run the **port-tagged vlan** command to join communications interfaces in the cluster to the management VLAN in trunk mode.

----End

## 3.10.8 Configuring Public Servers and Hosts for a Cluster

### Prerequisite

Do as follows on the administrator switch.

### Procedure

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

**Step 2** Run the **cluster** command to enter the cluster view.

**Step 3** Run the **ftp-server ip-address** command to configure a public FTP server for the cluster.

**Step 4** Run the **tftp-server ip-address** command to configure a public TFTP server for the cluster.

**Step 5** Run the **sftp-server ip-address** command to configure a public SFTP server for the cluster.

**Step 6** Run the **snmp-host ip-address** command to configure a public SNMP host for the cluster.

**Step 7** Run the **logging-host ip-address** command to configure a public log host for the cluster.

Member switches can access the servers and hosts that are configured through Steps 3 to 7 by accessing the administrator switch.

Steps 3 to 7 are optional and are not listed in sequence.

By default, no public server or host is configured for a cluster.

----End

## 3.10.9 Checking the Configuration

### Prerequisite

### Context

Run the following command to check the previous configuration.

| Action                                                           | Command                |
|------------------------------------------------------------------|------------------------|
| Check information about the cluster to which the device belongs. | <b>display cluster</b> |

## 3.11 Managing Switches in a Cluster Through HGMP

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

### [3.11.2 Sending Files to Member Switches in a Cluster in Batches](#)

### [3.11.3 Restarting Member Switches in a Cluster in Batches](#)

Restarting Member Switches in a Cluster in Batches

### [3.11.4 Enabling the Plug-and-Play Function](#)

Enabling the Plug-and-Play Function

### [3.11.5 Sending the Incremental Configuration](#)

Sending the Incremental Configuration

### [3.11.6 Synchronizing Configuration Files](#)

Synchronizing Configuration Files

### [3.11.7 Configuring Security Features](#)

Configuring Security Features

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

Checking the Configuration

## 3.11.1 Establishing the Configuration Task

### Applicable Environment

To optimize the performance parameters of the created cluster, you can manage switches in the cluster through HGMP to facilitate the management and maintenance of the cluster and better manage member switches in the cluster.

### Pre-configuration Tasks

A cluster is created by following the steps described in [3.4 Configuring a Cluster](#) and [3.8 Setting Parameters for a Cluster](#).

### Data Preparation

To configure NDP, you need the following data.

| No. | Data                                   |
|-----|----------------------------------------|
| 1   | Interval for sending handshake packets |
| 2   | Holdtime of packets                    |
| 3   | Aging time of member switches          |
| 4   | Multicast address of the cluster       |

| No. | Data                                                                                                                           |
|-----|--------------------------------------------------------------------------------------------------------------------------------|
| 5   | IP addresses of the public FTP server, TFTP server, SFTP server, log host, SNMP host used in the cluster                       |
| 6   | Default information about the FTP server that is configured for the cluster, including the IP address, user name, and password |

### 3.11.2 Sending Files to Member Switches in a Cluster in Batches

#### Prerequisite

Do as follows on the administrator switch.

#### Procedure

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

**Step 2** Run the **cluster** command to enter the cluster view.

**Step 3** (Optional) Run the **cluster-plug-play ip ip-address username user-name password password** command to configure default FTP login information.

After this command is run, configured information is used by default during the process of sending files to member switches in a cluster in batches.

**Step 4** Run the **cluster-member [ group-by { device-type type-name | ip { ip-address [ to ip-address ] } &<1-10> | member-number { member-number [ to member-number ] } &<1-10> } get { configuration-file | system-software | patch | license } { file-name } [ ip ip-address username user-name password password ]** command to send files to member switches in the cluster in batches.

- During the process of sending files to member switches in the cluster in batches, **group-by** can be used to specify member switch groups according to different selection modes.
- If Step 3 is not performed, you must enter the IP address, user name, and password when using this command.
- If Step 3 is performed, the IP address, user name, and password configured in Step 3 are used by default.
- IP addresses used in sending files to member switches in the cluster in batches are IP addresses used in the cluster.

----End

### 3.11.3 Restarting Member Switches in a Cluster in Batches

Restarting Member Switches in a Cluster in Batches

Do as follows on the administrator switch.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **cluster** command to enter the cluster view.
- Step 3** Run the **cluster-member reboot** [ **group-by** { **device-type** *type-name* | **ip** { *ip-address* [ **to** *ip-address* ] } &<1-10> | **member-number** { *member-number* [ **to** *member-number* ] } &<1-10> ] command to restart member switches in the cluster in batches.

The current configuration of the device is not saved during the process of restarting member switches in the cluster in batches.

----End

### 3.11.4 Enabling the Plug-and-Play Function

Enabling the Plug-and-Play Function

Do as follows on the administrator switch.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **cluster** command to enter the cluster view.
- Step 3** (Optional) Run the **cluster-plug-play ip** *ip-address* **username** *user-name* **password** *password* command to configure default FTP login information.
- Step 4** Run the **cluster-plug-play enable** command to enable the plug-and-play function.

Step 3 is performed in the scenario of replacing a device. The new device automatically downloads the configuration files of the old device. Prerequisites for the operation is that configuration files of the old device exist on the FTP server and the physical topologies and types of the new device and old device are the same.

----End

### 3.11.5 Sending the Incremental Configuration

Sending the Incremental Configuration

Do as follows on the administrator switch.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **cluster** command to enter the cluster view.
- Step 3** Run the **increment** command to enter the incremental configuration view.
- Step 4** Run the **increment-command** [ **command-number** *command-number* ] **command-text** *command-text* command to edit the command list.

**Step 5** Run the **increment-run** [ **group-by device-type** *type-name* | **ip** { *ip-address* [ **to ip-address** ] } &<1-10> | **member-number** { *member-number* [ **to member-number** ] } &<1-10> ] command to display the result whether commands in the command list are sent to the specified member switches.

- Only the last execution result of the incremental configuration is saved.
- The mode of member group selection can be member switch ID-based, device type-based, IP address-based, or all.
- If you use the ID of an existing command during the process of editing the command list, the command corresponding to the ID is overwritten.
- To delete the existing incremental configuration command, run the **undo increment-command** { **command-number** *command-number* | **all** } command.
- To view the list of incremental configuration commands that is edited, run the **display increment-command** command.

----End

## 3.11.6 Synchronizing Configuration Files

Synchronizing Configuration Files

### Prerequisite

Do as follows on the administrator switch.

### Procedure

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

**Step 2** Run the **cluster** command to enter the cluster view.

**Step 3** Run the **increment-config synchronization** [ **group-by** { **device-type** *type-name* | **ip** { *ip-address* [ **to ip-address** ] } &<1-10> | **member-number** { *member-number* [ **to member-number** ] } &<1-10> ] command to synchronize configuration files of the specified member switches with the FTP server.

- The mode of member group selection can be member switch ID-based, device type-based, IP address-based, or all.

----End

## 3.11.7 Configuring Security Features

Configuring Security Features

Do as follows on the administrator switch.

### Procedure

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

**Step 2** Run the **cluster** command to enter the cluster view.

**Step 3** Run the **cluster-member unrelated-port** [ **group-by** { **device-type** *type-name* | **ip** { *ip-address* [ **to** *ip-address* ] } &<1-10> | **member-number** { *member-number* [ **to** *member-number* ] } &<1-10> } { **ndp** | **ntdp** } command to disable NDP or NTDP on unrelated interfaces.

- Only the last command execution result is saved.
- The mode of member group selection can be member switch ID-based, device type-based, IP address-based, or all.
- This command is valid only after the cluster function is enabled.

----End

## 3.11.8 Checking the Configuration

Checking the Configuration

### Prerequisite

Run the following commands to check the previous configuration.

| Action                                                                                                  | Command                                         |
|---------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| Check the result of sending the incremental configuration.                                              | <b>display cluster-increment-result</b>         |
| Check the cluster license.                                                                              | <b>display cluster-license</b>                  |
| Check the cluster topology.                                                                             | <b>display cluster-topology-info</b>            |
| Check information about the incremental configuration.                                                  | <b>display increment-command</b>                |
| Check the result of synchronizing configuration files of member switches with the FTP server.           | <b>display increment-synchronization-result</b> |
| Check whether member switches successfully download configuration files, version files, or patch files. | <b>display member-getfile-stat</b>              |
| Check the status of NDP or NTDP on unrelated interfaces of member switches.                             | <b>display member-interface-state</b>           |
| Check whether member switches are restarted successfully.                                               | <b>display member-reboot-stat</b>               |
| Check whether member switches successfully save the current configuration.                              | <b>display member-save-stat</b>                 |
| Check the result of member switches synchronizing configuration files with the FTP server.              | <b>display synchronization-result</b>           |

## 3.12 Configuration Examples

This section provides several configuration examples of a cluster.

### Context

[3.12.1 Example for Creating a Cluster](#)

[3.12.2 Example for Member Switches Accessing a Public FTP Server Through FTP](#)

[3.12.3 Example for Devices Outside the Cluster Accessing Member Switches Through FTP](#)

[3.12.4 Example for Sending Files to Member Switches in a Cluster in Batches](#)

[3.12.5 Example for Restarting Member Switches in a Cluster in Batches](#)

[3.12.6 Example for Configuring the Incremental Configuration](#)

[3.12.7 Example for Synchronizing Configuration Files](#)

[3.12.8 Example for Configuring Security Features](#)

### 3.12.1 Example for Creating a Cluster

#### Context

#### Networking Requirements

As shown in [Figure 3-1](#), the S-switches are used to set up a Layer 2 network. Because of too many S-switches in the network, it is inconvenient to maintain and manage the S-switches on site. In addition, it is a waste of IP addresses to assign a public IP address to each S-switch.

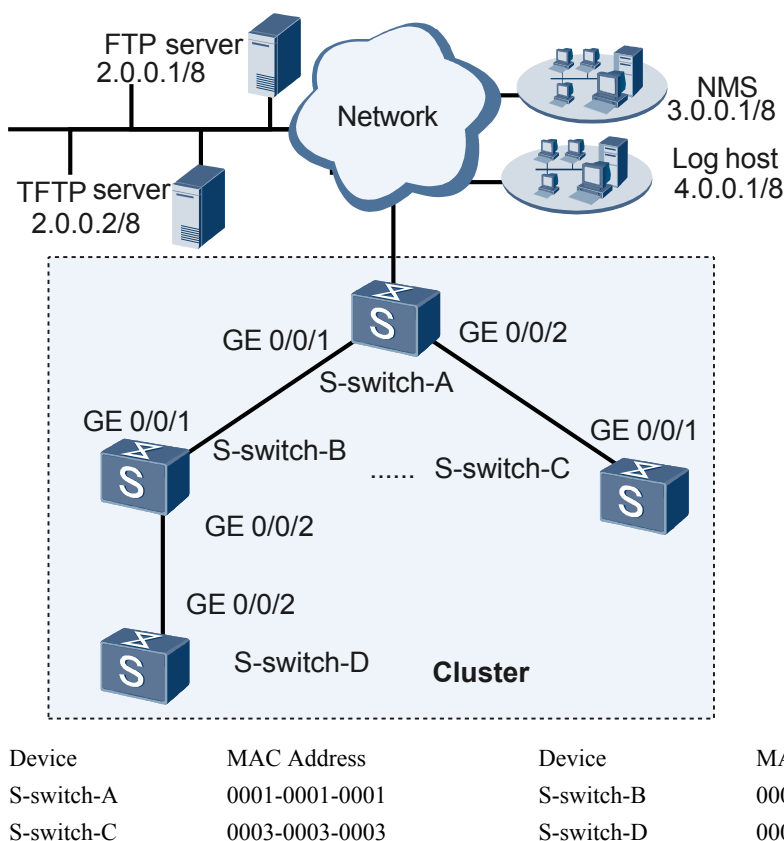
In this case, you can create a cluster for the Layer 2 network and manage the cluster through HGMP, thus effectively managing the Layer 2 network.

In this example, S-switch-A is the nearest to the network administrator and is configured as an administrator switch.

#### NOTE

For easy description, only four S-switches in the Layer 2 network are used in this example.

**Figure 3-1** Networking diagram for creating a cluster



## Configuration Roadmap

The configuration roadmap is as follows:

- Create the management VLAN on S-switch-A, S-switch-B, S-switch-C, and S-switch-D. Enable NDP and NTDP to ensure that each S-switch can discover network topologies by using NTDP.
- Choose the administrator switch, and then create cluster **HUAWEI** on the administrator switch.
- Add all the switches that support HGMP in the Layer 2 network to the cluster.
- Assign an IP address to VLANIF 1 to facilitate communications between member switches in the cluster and devices outside the cluster.
- Configure public servers and hosts for the cluster.

## Data Preparation

To complete the configuration, you need the following data:

- The ID of the management VLAN is 1.
- The IP address of interface VLANIF 1 is 5.0.0.1/8.
- The IP address pool of the cluster is 10.0.0.0/8.
- The cluster IP address of S-switch-A is 10.0.0.1/8.
- MAC addresses of the S-switches are shown in [Figure 3-1](#).

- For IP addresses of servers and hosts, see [Figure 3-1](#).

## Configuration Procedure

### NOTE

In this example, only the commands related to the HGMP configuration are listed.

1. Configure a management VLAN.

# Create VLAN 1 on S-switch-A, S-switch-B, S-switch-C, and S-switch-D. Take the configuration on S-switch-A as an example.

```
<S-switch-A> system-view
[S-switch-A] vlan 1
```

# Set the default VLAN to VLAN 1 for GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 on S-switch-A, GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 on S-switch-B, GigabitEthernet 0/0/1 on S-switch-C, and GigabitEthernet 0/0/2 on S-switch-D. Take the configuration on GigabitEthernet 0/0/1 on S-switch-A as an example.

```
[S-switch-A-vlan1] port GigabitEthernet 0/0/1
[S-switch-A-vlan1] quit
[S-switch-A] interface vlanif 1
[S-switch-A-Vlanif1] quit
```

2. Set interfaces to allow BPDUs to pass through.

# Enable BPDU in system view.

```
[S-switch-A] bpdu enable
```

3. Configure NDP.

# Enable the system NDP on S-switch-A, S-switch-B, S-switch-C, and S-switch-D. Take the configuration on S-switch-A as an example.

```
[S-switch-A] ndp enable
```

# Enable NDP on GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 of S-switch-A, GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 of S-switch-B, GigabitEthernet 0/0/1 of S-switch-C, and GigabitEthernet 0/0/2 of S-switch-D. Take the configuration on GigabitEthernet 0/0/1 of S-switch-A as an example.

```
[S-switch-A] interface GigabitEthernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] ndp enable
[S-switch-A-GigabitEthernet0/0/1] quit
```

# Verify the configuration.

```
[S-switch-A] display ndp interface GigabitEthernet0/0/1 to 0/0/2
Interface: GigabitEthernet0/0/1
```

```
Status: Enabled, Pkts Snd: 10, Pkts Rvd: 10, Pkts Err: 0
```

```
Neighbor 1: Aging Time: 16(s)
```

```
MAC Address : 0002-0002-0002
```

```
Port Name : GigabitEthernet0/0/1
```

```
Software Ver: Version 5.30 (S5300 V100R002C02B050)
```

```
Device Name : S-switch-B
```

```
Port Duplex : FULL
```

```
Product Ver : S5300
```

```
Interface: GigabitEthernet0/0/2
```

```
Status: Enabled, Pkts Snd: 10, Pkts Rvd: 10, Pkts Err: 0
```

```
Neighbor 1: Aging Time: 16(s)
```

```
MAC Address : 0003-0003-0003
```

```
Port Name : GigabitEthernet0/0/1
```

```
Software Ver: Version 5.30 (S5300 V100R002C02B050)
```

```
Device Name : S-switch-C
```

```
Port Duplex : FULL
```

```
Product Ver : S5300
```

4. Configure NTDP.

# Enable NTDP on S-switch-A, S-switch-B, S-switch-C, and S-switch-D. Take the configuration on S-switch-A as an example.

```
[S-switch-A] ntdp enable
```

# Set the interval for NTDP collecting topologies to 10 minutes. Take the configuration on S-switch-A as an example.

```
[S-switch-A] ntdp timer 10
```

# Set the range for NTDP to collect topologies to 5 hops. Take the configuration on S-switch-A as an example.

```
[S-switch-A] ntdp hop 5
```

# Verify the configuration.

```
[S-switch-A] display ntdp
Info:NTDP is running. Hops : 5
Timer : 10 min
Hop Delay : 200 ms
Port Delay : 20 ms
Last collection total time: 0ms
```

# Enable NTDP on GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 of S-switch-A, GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 of S-switch-B, GigabitEthernet 0/0/1 of S-switch-C, and GigabitEthernet 0/0/2 of S-switch-D. Take the configuration on GigabitEthernet 0/0/1 of S-switch-A as an example.

```
[S-switch-A] interface GigabitEthernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] ntdp enable
[S-switch-A-GigabitEthernet0/0/1] quit
```

# Verify the configuration.

```
[S-switch-A] display ntdp device-list
0004-0004-0004 2 S5300
0003-0003-0003 1 S5300
0002-0002-0002 1 S5300
0001-0001-0001 0 S5300
```

#### 5. Enable the cluster function.

# Enable the cluster function. Take S-switch-A as an example.

```
[S-switch-A] cluster enable
```

#### 6. Create a cluster.

Perform this step only on S-switch-A.

# The range of IP addresses that can be assigned to S-switch-A is 10.0.0.0/8. Assign the IP address 10.0.0.1/8 to S-switch-A.

```
[S-switch-A] cluster
[S-switch-A-cluster] ip-pool 10.0.0.1 8
```

# Create cluster HUAWEI on S-switch-A.

```
[S-switch-A-cluster] build HUAWEI
[HUAWEI_0.S-switch-A-cluster]
```

# Verify the configuration.

```
[HUAWEI_0.S-switch-A-cluster] display cluster
Cluster name:"HUAWEI"

Role:Administrator switch
management vlan id : 1(default vlan)
cluster multicast mac address : 0180-c200-000a(default)
cluster autojoin : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP-Pool:10.0.0.1/8
No logging host configured
No SNMP host configured
```

```
No FTP server configured
No TFTP server configured
No SFTP server configured
cluster-member ftp-timeout : 1200 sec(default)
Cluster SNMP NAT capability : enabled
Cluster FTP NAT capability : disabled
```

```
4 member(s) in the cluster, and 0 of them down.
```

# Display candidate switches discovered by the administrator switch.

```
[HUAWEI_0.S-switch-A-cluster] display cluster candidates
MAC HOP IP PLATFORM
0004-0004-0004 2 S5300
0003-0003-0003 1 S5300
0002-0002-0002 1 S5300
```

#### 7. Add member switches.

Perform this step only on S-switch-A.

# Add all candidate switches to the cluster. Take the mode of automatically adding member switches as an example. To add member switches manually, see [3.6 Adding a Member Switch](#).

```
[HUAWEI_0.S-switch-A-cluster] auto-build
Collecting candidate list, please wait...
Candidate list:
Name Hops MAC Address Device
S-switch-B 1 0002-0002-0002 S5300
S-switch-C 1 0003-0003-0003 S5300
S-switch-D 2 0004-0004-0004 S5300
Add all to cluster?(Y/N) y
Info: Cluster auto-build Finish!
3 member(s) added successfully
```

# Verify the configuration.

```
[HUAWEI_0.S-switch-A-cluster] display cluster members
SN Device MAC Address Status Name
0 S5300 0001-0001-0001 Admin HUAWEI_0.S-switch-A
1 S5300 0002-0002-0002 Up HUAWEI_1.S-switch-B
2 S5300 0003-0003-0003 Up HUAWEI_2.S-switch-C
3 S5300 0004-0004-0004 Up HUAWEI_3.S-switch-D
```

#### 8. Assign an IP address to VLANIF 1.

To ensure communications between member switches in the cluster and devices outside the cluster, you need to assign an IP address to VLANIF 1 on the administrator switch.

# Assign an IP address to VLANIF 1.

```
[HUAWEI_0.S-switch-A] interface vlanif 1
[HUAWEI_0.S-switch-A-Vlanif1] ip address 5.0.0.1 8
[HUAWEI_0.S-switch-A-Vlanif1] quit
```

# Verify the configuration.

```
[HUAWEI_0.S-switch-A] display interface Vlanif 1
Vlanif1 current state : UP
Line protocol current state : UP
Description : HUAWEI, Quidway Series, Vlanif1 Interface, Route Port
The Maximum Transmit Unit is 1500 bytes
Internet Address is 5.0.0.1/8
Internet Address is 10.0.0.1/8 Cluster
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is
0001-0001-0001
```

#### 9. Configure static routes.

This ensures that a reachable route exists between the S-switch and servers or hosts.

#### 10. Configure public servers and hosts of the cluster.

# Configure the FTP server.

```
[HUAWEI_0.S-switch-A] cluster
[HUAWEI_0.S-switch-A-cluster] ftp-server 2.0.0.1

Configure the TFTP server.
[HUAWEI_0.S-switch-A-cluster] tftp-server 2.0.0.2

Configure the Simple Network Management Protocol (SNMP) host.
[HUAWEI_0.S-switch-A-cluster] snmp-host 3.0.0.1

Configure the log host.
[HUAWEI_0.S-switch-A-cluster] logging-host 4.0.0.1

Verify the configuration.
[HUAWEI_0.S-switch-A-cluster] display cluster
Cluster name:"HUAWEI"
Role:Administrator

management vlan id : 1(default vlan)
cluster multicast mac : 0180-c200-000a(default)
cluster autojoin : disabled

Handshake timer:10 sec
Handshake hold-time:60 sec
IP-Pool:10.0.0.1/8
Logging host:4.0.0.1
SNMP host:3.0.0.1
FTP server:2.0.0.1
TFTP server:2.0.0.2

4 member(s) in the cluster, and 0 of them down.
```

## Configuration Files

- Configuration file of S-switch-A

```
#
sysname HUAWEI_0.S-switch-A
#
vlan batch 1
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
bpdu enable
#
interface Vlanif1
ip address 5.0.0.1 255.0.0.0
#
interface GigabitEthernet0/0/1
port default vlan 1
ntdp enable
ndp enable
#
interface GigabitEthernet0/0/2
port default vlan 1
ntdp enable
ndp enable
#
cluster
ip-pool 10.0.0.1 255.0.0.0
build HUAWEI
add-member 1 mac-address 0002-0002-0002
add-member 2 mac-address 0003-0003-0003
add-member 3 mac-address 0004-0004-0004
ftp-server 2.0.0.1
tftp-server 2.0.0.2
logging-host 4.0.0.1
```

```
snmp-host 3.0.0.1
#
```

- Configuration file of S-switch-B

```
#
sysname HUAWEI_1.S-switch-B
#
vlan batch 1
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
bpdu enable
#
interface Vlanif1
#
interface GigabitEthernet0/0/1
port default vlan 1
ntdp enable
ndp enable
#
interface GigabitEthernet0/0/2
port default vlan 1
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#
```

- Configuration file of S-switch-C

```
#
sysname HUAWEI_2.S-switch-C
#
vlan batch 1
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
bpdu enable
#
interface Vlanif1
#
interface GigabitEthernet0/0/1
port default vlan 1
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#
```

- Configuration file of S-switch-D

```
#
sysname HUAWEI_3.S-switch-D
#
vlan batch 1
#
cluster enable
ntdp enable
ntdp hop 5
ntdp timer 10
ndp enable
bpdu enable
#
interface Vlanif1
```

```
#
interface GigabitEthernet0/0/2
port default vlan 1
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#
```

### 3.12.2 Example for Member Switches Accessing a Public FTP Server Through FTP

#### Context

#### Networking Requirements

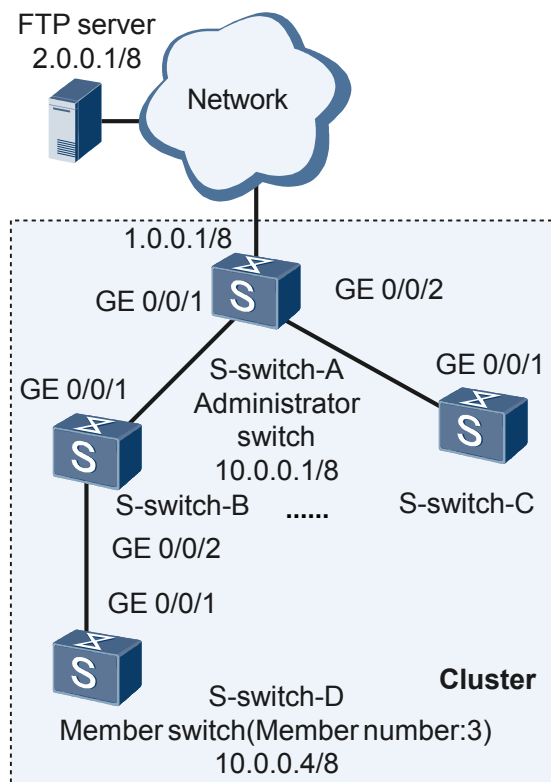


You can configure member switches to access a public FTP server through FTP in this same manner as configuring member switches to access a public TFTP server through TFTP.

As shown in [Figure 3-2](#), S-switch-A, S-switch-B, S-switch-C, and S-switch-D belong to the same cluster. S-switch-A is the administrator switch. S-switch-B, S-switch-C, and S-switch-D are member switches. The member ID of S-switch-D is 3.

It is required that files be uploaded to or downloaded from S-switch-B, S-switch-C, and S-switch-D. In this case, you can set a public FTP server for the cluster so that a member switch can log in to the FTP server and set up an FTP connection through the **cluster-ftp** command.

**Figure 3-2** Networking diagram for accessing a public FTP server



## Configuration Roadmap

The configuration roadmap is as follows:

- Create a cluster. For details, see section "[3.12.1 Example for Creating a Cluster](#)."
- Run the **cluster-ftp** command on a member switch to connect the member switch to the public FTP server.

## Data Preparation

To complete the configuration, you need the following data:

- The IP address of the VLANIF interface of the management VLAN is 5.0.0.1/8, which is reachable to the FTP server.
- The IP address pool of the cluster is 10.0.0.0/8.
- The cluster IP address of S-switch-A is 10.0.0.1/8.

## Configuration Procedure

### NOTE

In this example, only the commands related to the HGMP configuration are listed.

1. Create a cluster and configure cluster parameters and the FTP server.  
For details, see section "[3.12.1 Example for Creating a Cluster](#)."
2. Connect member switches to the public FTP server. Take the configuration on S-switch-D as an example.

```
<S-switch-D> cluster-ftp
Trying 10.0.0.1 ...
Press CTRL+K to abort
Connected to 10.0.0.1.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(10.0.0.1:(none)): User002
331 Give me your password, please
Password: *****
230 Logged in successfully
[ftp]
```

## Configuration Files

For details, see section "[3.12.1 Example for Creating a Cluster](#)."

## 3.12.3 Example for Devices Outside the Cluster Accessing Member Switches Through FTP

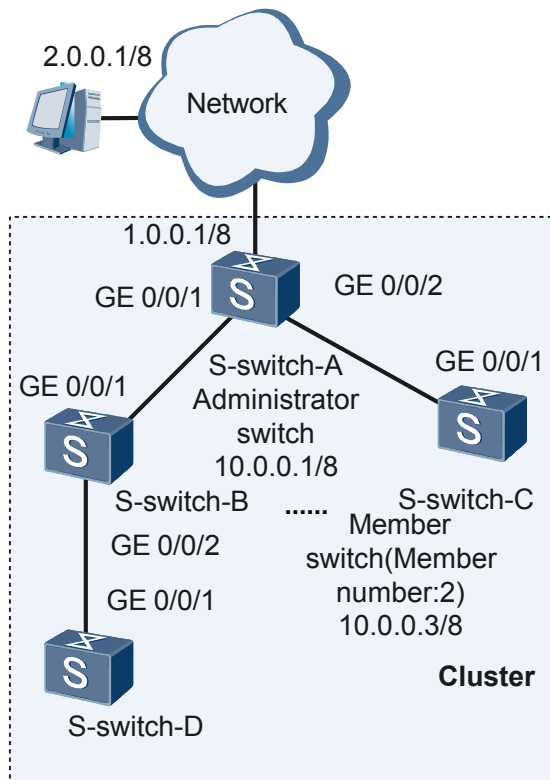
### Context

### Networking Requirements

As shown in [Figure 3-3](#), S-switch-A, S-switch-B, S-switch-C, and S-switch-D belong to the same cluster. S-switch-A is the administrator switch. S-switch-B, S-switch-C, and S-switch-D are member switches. The member ID of S-switch-C is 2.

It is required that files be uploaded to or downloaded from S-switch-B, S-switch-C, and S-switch-D. In this case, you can set up FTP connections between devices outside the cluster and member switches in the cluster through the network address translation (NAT).

**Figure 3-3** Networking diagram for devices accessing S-switch-C through FTP



## Configuration Roadmap

The configuration roadmap is as follows:

- Create a cluster. For details, see section "[3.12.1 Example for Creating a Cluster.](#)"
- Calculate the number of the interfaces that are reserved and used by member switches in the cluster to set up FTP connections.
- On a personal computer (PC), set up an FTP connection with a member switch through the FTP client.

## Data Preparation

To complete the configuration, you need the following data:

- The IP address of the management VLAN interface is 5.0.0.1/8.
- The IP address pool of the cluster is 10.0.0.0/8.
- The member ID of S-switch-C is 2.

## Configuration Procedure

### NOTE

In this example, only the commands related to the HGMP configuration are listed.

1. Create a cluster, and then configure cluster parameters.  
For details, see section "[3.12.1 Example for Creating a Cluster](#)."
2. Calculate the number of the interface that is reserved and used by member switches in the cluster to set up FTP connections.
3. Run the FTP client program on the PC and set up an FTP connection with S-switch-C through NAT.  

```
ftp> open 5.0.0.1 53252
Connected to 5.0.0.1.
220 FTP service ready.
User (5.0.0.1:(none)): User001
331 Password required for User001.
Password: *****
230 User logged in.
ftp>
```

## Configuration Files

For details, see section "[Configuration Files](#)."

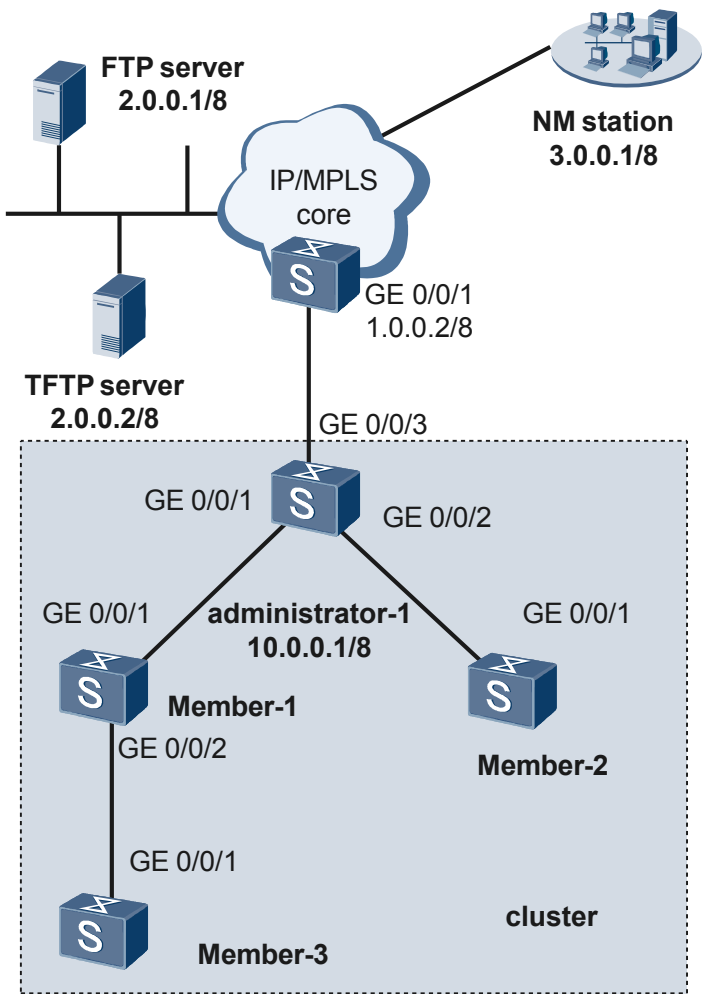
### 3.12.4 Example for Sending Files to Member Switches in a Cluster in Batches

#### Networking Requirements

As shown in [Figure 3-4](#), all the Layer 2 switches belong to the same cluster. Administrator-1 is the administrator switch of the cluster and other switches are member switches. The member ID of Member-2 is 2 and the member ID of Member-3 is 3.

Member-2 and Member-3 are required to download configuration files in batches from the FTP server.

Figure 3-4 Networking diagram for sending files to member switches in a cluster in batches



| Device          | MAC Address    | Device   | MAC Address    |
|-----------------|----------------|----------|----------------|
| Administrator-1 | 0001-0001-0001 | Member-1 | 0002-0002-0002 |
| Member-2        | 0003-0003-0003 | Member-3 | 0004-0004-0004 |

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a cluster by following the steps described in [3.4 Configuring a Cluster](#) and [3.8 Setting Parameters for a Cluster](#).
2. Configure that member switches access a public FTP server through FTP. For details, see [3.12.2 Example for Member Switches Accessing a Public FTP Server Through FTP](#).

NOTE

- If the system software files, patch files, license files, or configuration files are sent to member switches in a cluster in batches without accessing the FTP server outside the cluster, you can skip this step.
3. Send files to member switches in the cluster in batches on the administrator switch.

Data Preparation

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 1 by default.
- IP address of VLANIF 1 that is 5.0.0.1/8 and a reachable route between VLANIF 1 and the FTP server.
- Address pool of the cluster, that is 10.0.0.0/8.
- IP address of the administrator switch used in the cluster, that is 10.0.0.1/8.
- Member ID of Member-2 being 2 and member ID of Member-3 being 3.

## Configuration Procedure

1. Create a cluster, and then set parameters for the cluster.  
For details, see [3.4 Configuring a Cluster](#) and [3.8 Setting Parameters for a Cluster](#).
2. Configure the interconnection between the FTP server and devices in and outside the HGMP cluster.  
For details, see [3.12.2 Example for Member Switches Accessing a Public FTP Server Through FTP](#).

3. Send files to member switches in the cluster in batches.  
# Run the command for sending files to member switches in batches on the administrator switch. Member switches download configuration files from the FTP server 2.0.0.1 in NAT mode and automatically set them as the default configuration files for the next startup.

4. Verify the configuration.  
# Run the **display member-getfile-stat** command on the administrator switch to check whether member switches successfully download the configuration files, system software, and patch files. The command output shows that **succeed** is displayed.

```
[HUAWEI_0.Administrator-1] display member-getfile-stat
The status of member switchs getting file:
```

| SN | Device | MacAddress     | IPAddress | Result  |
|----|--------|----------------|-----------|---------|
| 2  | S5300  | 0003-0003-0003 | 10.0.0.3  | Succeed |
| 3  | S5300  | 0004-0004-0004 | 10.0.0.4  | Succeed |

# Run the **dir** command on member switches. The command output shows that member switches successfully download the specified configuration files. Take Member-2 as an example.

```
<HUAWEI_2.Member-2> dir *.zip
Directory of cfcad:/
```

| Idx | Attr | Size(Byte) | Date        | Time     | FileName        |
|-----|------|------------|-------------|----------|-----------------|
| 0   | -rw- | 1,491      | Sep 03 2008 | 17:43:52 | vrpcfg.zip      |
| 1   | -rw- | 752        | Aug 05 2008 | 15:04:36 | vrpcfg-hgmp.zip |

506,880 KB total (35,920 KB free)

```
<HUAWEI_2.Member-2> cd slave#cfcad:
```

```
<HUAWEI_2.Member-2> dir *.zip
```

```
Directory of slave#cfcad:/
```

| Idx | Attr | Size(Byte) | Date        | Time     | FileName        |
|-----|------|------------|-------------|----------|-----------------|
| 0   | -rw- | 1,491      | Sep 03 2008 | 17:43:54 | vrpcfg.zip      |
| 1   | -rw- | 752        | Aug 05 2008 | 15:07:50 | vrpcfg-hgmp.zip |

503,544 KB total (34,776 KB free)

# Run the **display startup** command on member switches. The command output shows that names of the configuration files for the next startup of member switches are changed. Take Member-2 as an example.

```
<HUAWEI_2.Member-2> display startup
```

```
MainBoard:
```

```
Configured startup system software: cfcad:/3328.cc
```

```

Startup system software: cfcard:/3328.cc
Next startup system software: cfcard:/3328.cc
Startup saved-configuration file: cfcard:/vrpcfg.zip
Next startup saved-configuration file: cfcard:/vrpcfg-hgmp.zip
Startup license file: NULL
Next startup license file: NULL
Startup patch package: NULL
Next startup patch package: NULL
SlaveBoard:
Configured startup system software: cfcard:/3328.cc
Startup system software: cfcard:/3328.cc
Next startup system software: cfcard:/3328.cc
Startup saved-configuration file: cfcard:/vrpcfg.zip
Next startup saved-configuration file: cfcard:/vrpcfg-hgmp.zip
Startup license file: NULL
Next startup license file: NULL
Startup patch package: NULL
Next startup patch package: NULL

```

## Configuration Files

- Configuration file of Administrator-1

```

#
sysname HUAWEI_0.Administrator-1

#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10
#
interface Vlanif1
ip address 5.0.0.1 255.0.0.0

#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet 0/0/2
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet 0/0/3
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
ip pool 10.0.0.1 255.0.0.0
build HUAWEI
add-member 1 mac-address 0002-0002-0002
add-member 2 mac-address 0003-0003-0003
add-member 3 mac-address 0004-0004-0004
ftp-server 2.0.0.1 255.0.0.0

```

```
tftp-server 2.0.0.2 255.0.0.0
snmp-host 3.0.0.1
```

- Configuration file of Member-1

```
#
sysname HUAWEI_1.Member-1
#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface vlanif 1
#
interface GigabitEthernet 0/0/1
bpdu enable
port default vlan 1
ntdp enable
ndp enable
#
interface GigabitEthernet 0/0/2
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#
```

- Configuration file of Member-2

```
#
sysname HUAWEI_1.Member-2
#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface vlanif 1
#
interface GigabitEthernet 0/0/1
bpdu enable
port default vlan 1
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#
```

- Configuration file of Member-3

```
sysname HUAWEI_1.Member-3
#
```

```
vlan batch 1
#
 cluster
enable
 ntdp
enable
 ntdp hop
5
 ndp
enable
 ntdp timer 10

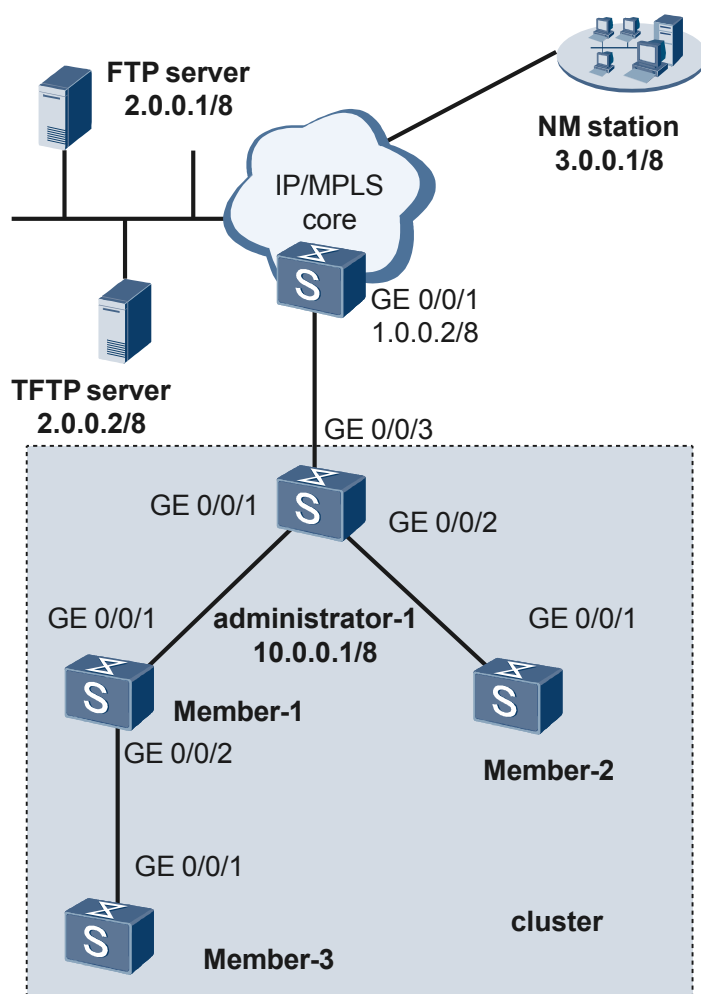
#
interface vlanif 1
#
 interface GigabitEthernet 0/0/1
 bpdu enable
 port default vlan 1
 ntdp enable
 ndp enable
#
cluster
 administrator-address 0001-0001-0001 name HUAWEI
#
```

### 3.12.5 Example for Restarting Member Switches in a Cluster in Batches

#### Networking Requirements

As shown in [Figure 3-5](#), all the Layer 2 switches belong to the same cluster. Administrator-1 is the administrator switch of the cluster and other switches are member switches. The member ID of Member-2 is 2 and the member ID of Member-3 is 3.

Member switches Member-2 and Member-3 are required to be restarted.

**Figure 3-5** Networking diagram for restarting member switches in a cluster in batches

| Device          | MAC Address    | Device   | MAC Address    |
|-----------------|----------------|----------|----------------|
| Administrator-1 | 0001-0001-0001 | Member-1 | 0002-0002-0002 |
| Member-2        | 0003-0003-0003 | Member-3 | 0004-0004-0004 |

## Configuration Roadmap

The configuration roadmap is as follows:

1. Create a cluster by following the steps described in [3.4 Configuring a Cluster](#) and [3.8 Setting Parameters for a Cluster](#).
2. Restart member switches in the cluster in batches on the administrator switch.

## Data Preparation

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 1 by default.
- IP address of VLANIF 1 that is 5.0.0.1/8 and a reachable route between VLANIF 1 and the FTP server.

- Address pool of the cluster, that is 10.0.0.0/8.
- IP address of the administrator switch used in the cluster, that is 10.0.0.1/8.
- Member ID of Member-2 being 2 and member ID of Member-3 being 3.

## Context

1. Create a cluster, and then set parameters for the cluster.  
For details, see [3.4 Configuring a Cluster](#) and [3.8 Setting Parameters for a Cluster](#).
2. Restart member switches in the cluster in batches.  
# Run the command for restarting member switches in the cluster in batches on the administrator switch to restart Member-2 and Member-3.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-member reboot group-by member-
number 2 to 3
Info: This command will take members reboot.
Are you sure?[Y/N]y
```

3. Verify the configuration.  
# Run the **display member-reboot-stat** command on administrator switches to check whether the member switches are successfully restarted. The command output shows that **succeed** is displayed, which indicates that the specified member switches are restarted successfully.

```
[HUAWEI_0.Administrator-1] display member-reboot-stat
The result of member switchs rebooting:
```

| SN | Device | MacAddress     | IPAddress | Result         |
|----|--------|----------------|-----------|----------------|
| 1  | S5300  | 0003-0003-0003 | 10.0.0.3  | <b>Succeed</b> |
| 2  | S5300  | 0004-0004-0004 | 10.0.0.4  | <b>Succeed</b> |

## Configuration Files

- Configuration file of Administrator-1

```
#
sysname HUAWEI_0.Administrator-1

#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface Vlanif1
ip address 5.0.0.1 255.0.0.0

#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet 0/0/2
```

```

port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet 0/0/3
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
ip pool 10.0.0.0 255.0.0.0
build HUAWEI
add-member 1 mac-address 0002-0002-0002
add-member 2 mac-address 0003-0003-0003
add-member 3 mac-address 0004-0004-0004
ftp-server 2.0.0.1 255.0.0.0
tftp-server 2.0.0.2 255.0.0.0
snmp-host 3.0.0.1

```

- Configuration file of Member-1

```

#
sysname HUAWEI_1.Member-1
#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface vlanif 1
#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet 0/0/2
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#

```

- Configuration file of Member-2

```

#
sysname HUAWEI_1.Member-2
#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable

```

```

 ntdp timer 10

#
interface vlanif 1
#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#

```

- Configuration files of Member-3

```

sysname HUAWEI_1.Member-3
#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface vlanif 1
#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#

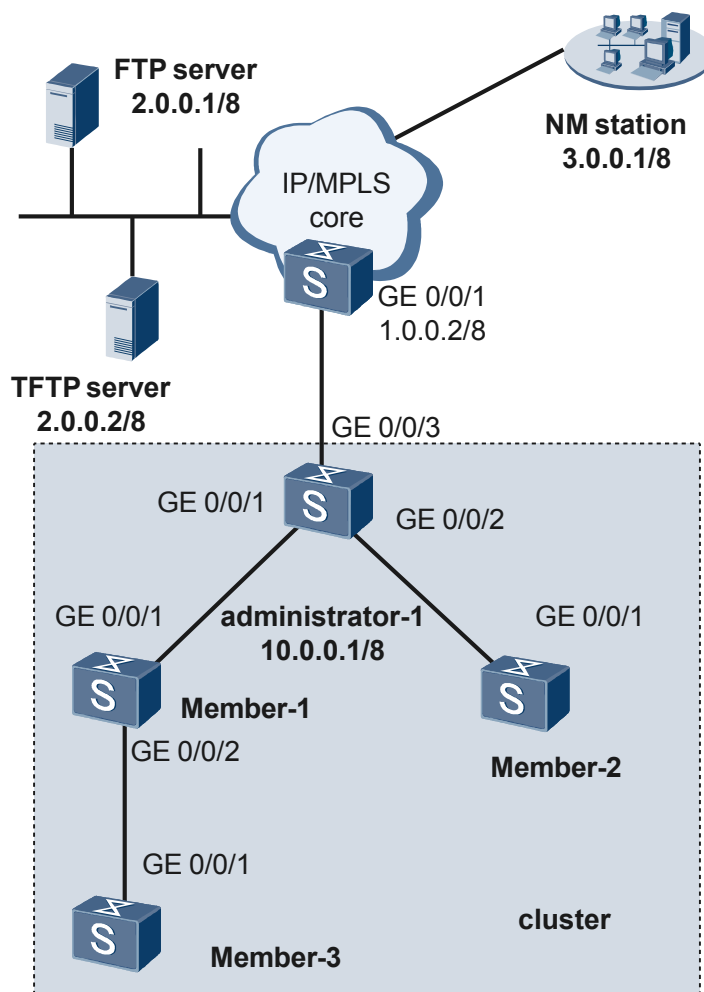
```

## 3.12.6 Example for Configuring the Incremental Configuration

### Networking Requirements

As shown in [Figure 3-6](#), all the Layer 2 switches belong to the same cluster. Administrator-1 is the administrator switch of the cluster and other switches are member switches. The member ID of Member-2 is 2 and the member ID of Member-3 is 3.

It is required to create VLAN 10 to VLAN 20 on Member-2 and Member-3 and configure the next hop address as the static route of the administrator switch. In this case, you can use the incremental configuration function of the HGMP cluster.

**Figure 3-6** Networking diagram for configuring the incremental configuration function for an HGMP cluster

| Device          | MAC Address    | Device   | MAC Address    |
|-----------------|----------------|----------|----------------|
| Administrator-1 | 0001-0001-0001 | Member-1 | 0002-0002-0002 |
| Member-2        | 0003-0003-0003 | Member-3 | 0004-0004-0004 |

## Configuration Roadmap

The configuration roadmap is as follows:

1. Create a cluster by following the steps described in [3.4 Configuring a Cluster](#) and [3.8 Setting Parameters for a Cluster](#).
2. Edit the list of incremental configuration commands on the administrator switch.
3. Send the list of incremental configuration commands to the specified member switches.

## Data Preparation

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 1 by default.

- IP address of VLANIF 1 that is 5.0.0.1/8 and a reachable route between VLANIF 1 and the FTP server.
- Address pool of the cluster, that is 10.0.0.0/8.
- IP address of the administrator switch used in the cluster, that is 10.0.0.1/8.
- Member ID of Member-2 being 2 and member ID of Member-3 being 3.

## Configuration Procedure

1. Create a cluster, and then set parameters for the cluster.  
For details, see [3.12.1 Example for Creating a Cluster](#).
2. Edit the list of incremental configuration commands on the administrator switch.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] increment
[HUAWEI_0.Administrator-1-cluster-increment] increment-command command-number
10 command-text vlan batch 10 to 20
[HUAWEI_0.Administrator-1-cluster-increment] increment-command command-number
20 command-text ip route-static 2.0.0.0 8 10.0.0.1
```

After the previous configuration is complete, run the **display increment-command** command on the administrator switch to view the list of incremental configuration commands.

```
[HUAWEI_0.Administrator-1-cluster-increment] display increment-command
The content of increment commands:
```

| SN | Content                            |
|----|------------------------------------|
| 10 | vlan batch 10 to 20                |
| 20 | ip route-static 2.0.0.0 8 10.0.0.1 |

3. Send the list of incremental configurations command to the specified member switches.  
[HUAWEI\_0.Administrator-1-cluster-increment-cluster-increment] **increment-run group-by member-number 2 to 3**
4. Verify the configuration.

Run the **display cluster-increment-result** command on administrator to check whether the list of incremental configuration commands is sent to the specified member switches. The command output shows that **success** is displayed.

```
[HUAWEI_0.Administrator-1-cluster-increment] display cluster-increment-result
The result of member switchs executing increment commands:
```

| SN | Device | MacAddress     | IpAddress | Result  | CommandId |
|----|--------|----------------|-----------|---------|-----------|
| 2  | S5300  | 0003-0003-0003 | 10.0.0.3  | success | -         |
| 3  | S5300  | 0004-0004-0004 | 10.0.0.4  | success | -         |

## Context

- Configuration file of Administrator-1  
#  
sysname HUAWEI\_0.Administrator-1

```

#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface Vlanif1
ip address 5.0.0.1 255.0.0.0

#
interface GigabitEthernet 0/0/1
port default vlan 1
ntdp enable
ndp enable
#
interface GigabitEthernet 0/0/2
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet 0/0/3
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
ip pool 10.0.0.0 255.0.0.0
build HUAWEI
add-member 1 mac-address 0002-0002-0002
add-member 2 mac-address 0003-0003-0003
add-member 3 mac-address 0004-0004-0004
ftp-server 2.0.0.1 255.0.0.0
tftp-server 2.0.0.2 255.0.0.0
snmp-host 3.0.0.1

```

- Configuration files of Member-1

```

#
sysname HUAWEI_1.Member-1
#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface vlanif 1
#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable

```

```
#
interface GigabitEthernet 0/0/2
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#
```

- Configuration file of Member-2

```
#
sysname HUAWEI_1.Member-2
#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface vlanif 1
#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#
```

- Configuration files of Member-3

```
sysname HUAWEI_1.Member-3
#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface vlanif 1
#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#
```

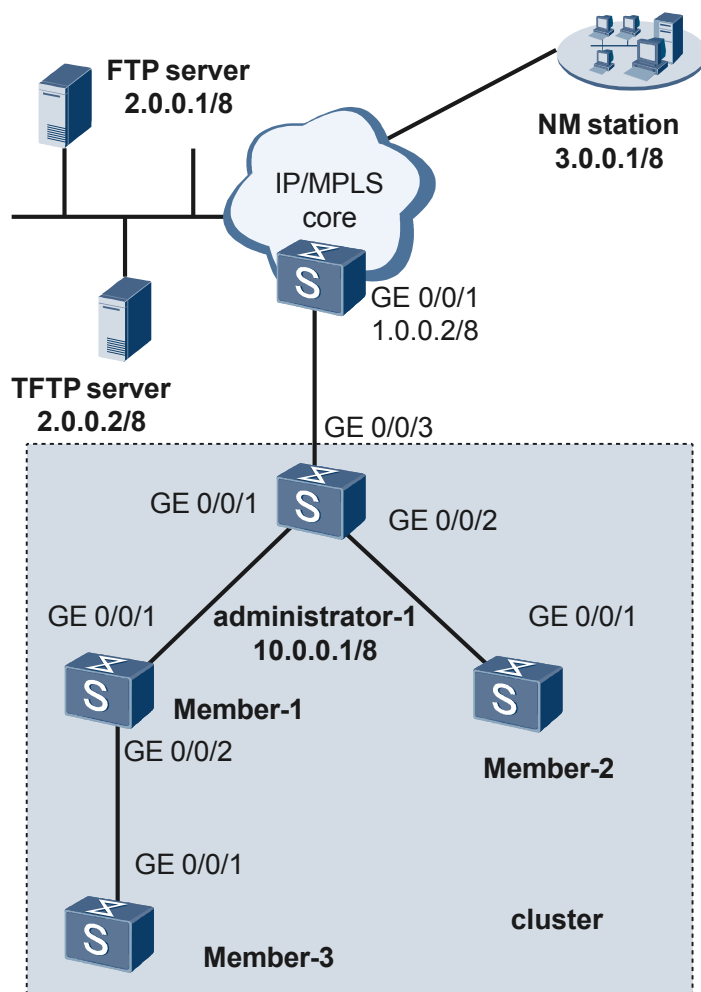
### 3.12.7 Example for Synchronizing Configuration Files

#### Networking Requirements

As shown in [Figure 3-7](#), all the Layer 2 switches belong to the same cluster. Administrator-1 is the administrator switch of the cluster and other switches are member switches. The member ID of Member-2 is 2 and the member ID of Member-3 is 3.

It is required to synchronize configuration files of all member switches with the FTP server.

**Figure 3-7** Networking diagram for synchronizing configuration files for an HGMP cluster



| Device          | MAC Address    | Device   | MAC Address    |
|-----------------|----------------|----------|----------------|
| Administrator-1 | 0001-0001-0001 | Member-1 | 0002-0002-0002 |
| Member-2        | 0003-0003-0003 | Member-3 | 0004-0004-0004 |

#### Configuration Roadmap

The configuration roadmap is as follows:

1. Create a cluster by following the steps described in [3.4 Configuring a Cluster](#) and [3.8 Setting Parameters for a Cluster](#).
2. Configure that member switches access a public FTP server through FTP. For details, see [3.12.2 Example for Member Switches Accessing a Public FTP Server Through FTP](#).

 **NOTE**

If the system software files, patch files, license files, or configuration files are sent to member switches in a cluster in batches without accessing the FTP server outside the cluster, you can skip this step.

3. Send files to member switches in the cluster in batches on the administrator switch.

## Data Preparation

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 1 by default.
- IP address of VLANIF 1 that is 5.0.0.1/8 and a reachable route between VLANIF 1 and the FTP server.
- Address pool of the cluster, that is 10.0.0.0/8.
- IP address of the administrator switch used in the cluster, that is 10.0.0.1/8.
- Member ID of Member-2 being 2 and member ID of Member-3 being 3.

## Configuration Procedure

1. Create a cluster, and then set parameters for the cluster.  
For details, see [3.4 Configuring a Cluster](#) and [3.8 Setting Parameters for a Cluster](#).
2. Configure the interconnection between the FTP server and devices in and outside the HGMP cluster.

For details, see [3.12.2 Example for Member Switches Accessing a Public FTP Server Through FTP](#).

3. Synchronize configuration files.  
# Run the command for synchronizing configuration files on the administrator switch, and then member switches synchronize configuration files with the FTP server 2.0.0.1 in NAT mode.

```
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] cluster-plugin-play ip 2.0.0.1 username hgmp
password hgmp
[HUAWEI_0.Administrator-1-cluster] increment-config synchronization
```

4. Verify the configuration.  
# After the previous configuration is complete, run the **display increment-synchronization-result** command on administrator to check whether configuration files are synchronized with the FTP server. The command output shows that **success** is displayed.

```
[HUAWEI_0.Administrator-1-cluster-increment] display increment-synchronization-result
```

The result of member switches' synchronization:

| SN | Device | MacAddress     | IpAddress | result  |
|----|--------|----------------|-----------|---------|
| 1  | S5300  | 0002-0002-0002 | 10.0.0.2  | success |
| 2  | S5300  | 0003-0003-0003 | 10.0.0.3  | success |
| 3  | S5300  | 0004-0004-0004 | 10.0.0.4  | success |

On the FTP server, you can view that the names of configuration files are the MAC address of member switches, which indicates that configuration files in the HGMP cluster are synchronized.

## Configuration Files

- Configuration file of Administrator-1

```
#
sysname HUAWEI_0.Administrator-1

#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ndp timer hello 125
ndp timer aging 200
#
interface Vlanif1
ip address 5.0.0.1 255.0.0.0

#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet 0/0/2
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet 0/0/3
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
ip pool 10.0.0.0 255.0.0.0
build HUAWEI
add-member 1 mac-address 0002-0002-0002
add-member 2 mac-address 0003-0003-0003
add-member 3 mac-address 0004-0004-0004
ftp-server 2.0.0.1 255.0.0.0
tftp-server 2.0.0.2 255.0.0.0
snmp-host 3.0.0.1
```

- Configuration file of Member-1

```
#
sysname HUAWEI_1.Member-1
#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
```

```
ndp
enable
ndp timer hello 125
ndp timer aging 200

#
interface vlanif 1
#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet 0/0/2
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#
```

- Configuration file of Member-2

```
#
sysname HUAWEI_1.Member-2
#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface vlanif 1
#
interface GigabitEthernet 0/0/1
port default vlan
bpdu enable1
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#
```

- Configuration file of Member-3

```
sysname HUAWEI_1.Member-3
#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface vlanif 1
```

```
#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#
```

## 3.12.8 Example for Configuring Security Features

### Networking Requirements

As shown in [Figure 3-8](#), all the Layer 2 switches belong to the same cluster. Administrator-1 is the administrator switch of the cluster and other switches are member switches. The member ID of Member-2 is 2 and the member ID of Member-3 is 3.

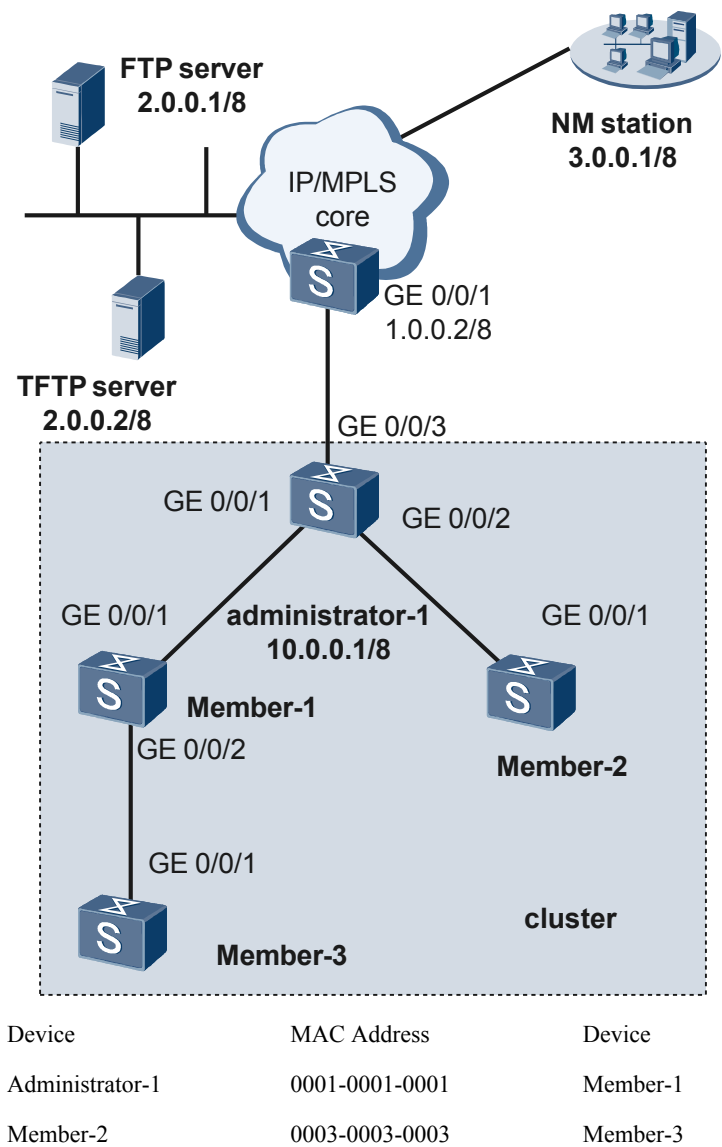
It is required to disable NDP and NTDP on the interfaces of all the member switches that do not need NDP or NTDP. To improve the security of the HGMP cluster, you can configure security features for the HGMP cluster.



#### NOTE

After NDP or NTDP is disabled on unrelated interfaces of member switches, if the new candidate switches access these unrelated interfaces, they cannot join the cluster until NDP or NTDP is enabled.

Figure 3-8 Networking diagram for configuring security features for an HGMP cluster



Configuration Roadmap

The configuration roadmap is as follows:

1. Create a cluster by following the steps described in [3.4 Configuring a Cluster](#) and [3.8 Setting Parameters for a Cluster](#).
2. On the administrator switch, run the command for disabling NDP and NTDP on unrelated interfaces of member switches.

Data Preparation

To complete the configuration, you need the following data:

- Management VLAN ID of the cluster, that is 1 by default.
- IP address of VLANIF 1 that is 5.0.0.1/8 and a reachable route between VLANIF 1 and the FTP server.

- Address pool of the cluster, that is 10.0.0.0/8.
- IP address of the administrator switch used in the cluster, that is 10.0.0.1/8.
- Member ID of Member-2 being 2 and member ID of Member-3 being 3.

## Configuration Procedure

1. Create a cluster, and then set parameters for the cluster.

For details, see [3.4 Configuring a Cluster](#) and [3.8 Setting Parameters for a Cluster](#).

2. Disable NDP and NTDP.

# Disable NDP and NTDP on interfaces of all the member switches that do not need NDP and NTDP.

```
Disable NDP on the unrelated interfaces of member switches
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] undo cluster-member unrelated-port ndp
Disable NTDP on the unrelated interfaces of member switches
[HUAWEI_0.Administrator-1] cluster
[HUAWEI_0.Administrator-1-cluster] undo cluster-member unrelated-port ntdp
```

3. Verify the configuration.

After the previous configuration, run the **display member-interface-state** command on administrator to check whether NDP or NTDP is disabled on unrelated interfaces of the member switches, and you can view that **success** is displayed.

```
[HUAWEI_0.Administrator-1-cluster] display member-interface-state ndp
The result of member switches executed disable member interface command:
```

| SN | Device | MacAddress     | IpAddress | result  |
|----|--------|----------------|-----------|---------|
| 3  | S5300  | 0004-0004-0004 | 10.0.0.4  | success |
| 2  | S5300  | 0003-0003-0003 | 10.0.0.3  | success |
| 1  | S5300  | 0002-0002-0002 | 10.0.0.2  | success |

```
[HUAWEI_0.Administrator-1-cluster] display member-interface-state ntdp
The result of member switches executed disable member interface command:
```

| SN | Device | MacAddress     | IpAddress | result  |
|----|--------|----------------|-----------|---------|
| 3  | S5300  | 0004-0004-0004 | 10.0.0.4  | success |
| 2  | S5300  | 0003-0003-0003 | 10.0.0.3  | success |
| 1  | S5300  | 0002-0002-0002 | 10.0.0.2  | success |

## Configuration Files

- Configuration file of Administrator-1

```
#
sysname HUAWEI_0.Administrator-1

#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface Vlanif1
```

```
ip address 5.0.0.1 255.0.0.0

#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet 0/0/2
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet 0/0/3
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
ip pool 10.0.0.0 255.0.0.0
build HUAWEI
add-member 1 mac-address 0002-0002-0002
add-member 2 mac-address 0003-0003-0003
add-member 3 mac-address 0004-0004-0004
ftp-server 2.0.0.1 255.0.0.0
tftp-server 2.0.0.2 255.0.0.0
snmp-host 3.0.0.1
```

- Configuration file of Member-1

```
#
sysname HUAWEI_1.Member-1
#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface vlanif 1
#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
interface GigabitEthernet 0/0/2
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#
```

- Configuration file of Member-2

```
#
sysname HUAWEI_1.Member-2
#
```

```
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface vlanif 1
#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#
```

- Configuration file of Member-3

```
sysname HUAWEI_1.Member-3
#
vlan batch 1
#
cluster
enable
ntdp
enable
ntdp hop
5
ndp
enable
ntdp timer 10

#
interface vlanif 1
#
interface GigabitEthernet 0/0/1
port default vlan 1
bpdu enable
ntdp enable
ndp enable
#
cluster
administrator-address 0001-0001-0001 name HUAWEI
#
```

# 4 LLDP Configuration

---

## About This Chapter

This chapter describes the basics of the Link Layer Discovery Protocol (LLDP) and how to configure LLDP.

### [4.1 Introduction](#)

This section describes the principle and concepts of LLDP.

### [4.2 Configuring LLDP](#)

This section describes how to configure LLDP.

### [4.3 Maintaining LLDP](#)

This section describes how to maintain and debug LLDP.

### [4.4 Configuration Examples](#)

This section provides several configuration examples of LLDP.

## 4.1 Introduction

This section describes the principle and concepts of LLDP.

### [4.1.1 LLDP Overview](#)

### [4.1.2 Basic Concepts](#)

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

## 4.1.1 LLDP Overview

### Background

At present, the Ethernet technology is extensively used in the Local Area Network (LAN) and Metropolitan Area Network (MAN). With the increasing demand for large-scale networks, the capabilities for the Network Management System (NMS) are in great demand. For example, the NMS should address issues such as obtaining topology of interconnected devices and conflicts in configurations on different devices.

Recently, the NMS software adopts the function of automated discovery to trace changes in topology. Most NMS software, however, can at best analyze the Layer 3 network topology and group devices to different IP subnets. The NMS provides data only about adding or deleting devices. The NMS cannot obtain information about the interfaces on a device, which are used to connect another device. That is, the NMS cannot locate a device or determine its operation mode.

### Introduction to LLDP

The Layer 2 Discovery (L2D) protocol can discover precise information about the interfaces situated on devices and the interfaces that are used to connect other devices. The L2D protocol also helps display the paths between the client, switch, router, application server, and network server. The preceding detailed information helps in finding the root cause of the network failure.

The LLDP protocol is an L2D protocol defined in IEEE 802.1ab. The LLDP protocol specifies that the status information is stored on all the interfaces, and the device can send its status information to the neighbor stations. The interfaces can also send information about changes in the status to the neighbor stations if required. The neighbor stations then store the received information in the standard Management Information Base (MIB) of the Simple Network Management Protocol (SNMP). The NMS can search for the Layer 2 information in the MIB. As specified in the IEEE 802.1ab standard, the NMS can also find unreasonable Layer 2 configurations based on information provided by LLDP.

When the LLDP protocol runs on devices, the NMS can obtain the Layer 2 information about all the devices it connects and detailed information about the network topology. This expands the scope of network management. LLDP also helps find unreasonable configurations on the network and reports the configurations to the NMS. This helps remove the errors in configurations timely.

## 4.1.2 Basic Concepts

### MIB

MIB stands for the Management Information Base. MIB consists of the LLDP local system MIB and the LLDP remote system MIB.

The LLDP local system MIB stores information about the local station, including the chassis ID, port ID, system name, system description, port description, system capabilities, and management address.

The LLDP remote system MIB stores information about adjacent stations, including the chassis ID, port ID, system name, system description, port description, system capabilities, and management address.

### LLDP Agent

An LLDP agent is the protocol entity that manages LLDP operations for an interface.

An LLDP agent performs the following tasks:

- Maintains current information in the LLDP local system MIB.
- Extracts and sends LLDP local system MIB information to neighbor stations when the status of the local device changes. An LLDP agent also extracts and sends LLDP local system MIB information to neighbor stations at regular intervals when no status change occurs on the local device.
- Identifies and processes received LLDP frames.
- Maintains current information in the LLDP remote system MIB.
- Sends LLDP traps to the NMS when a change occurs in the LLDP local system MIB or the LLDP remote system MIB.

### LLDP Management Address

The LLDP management address (hereinafter referred to as the management address) is used by the NMS to identify the S-switch and implement network management. The management address identifies a device. This facilitates the layout of the network topology and network management with a clear view of the topology status. The management address is carried in the management address Type-Length-Value (TLV) field in an LLDP frame to be transmitted to neighbor stations.

### LLDP Traps

When the LLDP local system MIB or the LLDP remote system MIB changes, the S-switch sends traps to the NMS for updating the topology. The traps can be triggered in the following cases:

- LLDP is enabled or disabled globally.
- The local management address changes.
- Neighbor information changes. A trap is not generated if the management address of the neighbor changes.

The LLDP trap function is of global significance for the S-switch. That is, it provides the trap function on all the interfaces.

## 4.1.3 Logical Relationships Between Configuration Tasks

In the chapter, all configuration tasks are optional and not listed in sequence. You can configure them as required.

## 4.2 Configuring LLDP

This section describes how to configure LLDP.

[4.2.1 Establishing the Configuration Task](#)

[4.2.2 \(Optional\) Enabling the LLDP Trap Function](#)

[4.2.3 Enabling LLDP on an Interface](#)

[4.2.4 \(Optional\) Disabling LLDP on an Interface](#)

[4.2.5 \(Optional\) Re-enabling LLDP on an Interface](#)

[4.2.6 \(Optional\) Setting the LLDP Management Address](#)

[4.2.7 \(Optional\) Setting LLDP Attributes](#)

[4.2.8 Checking the Configuration](#)

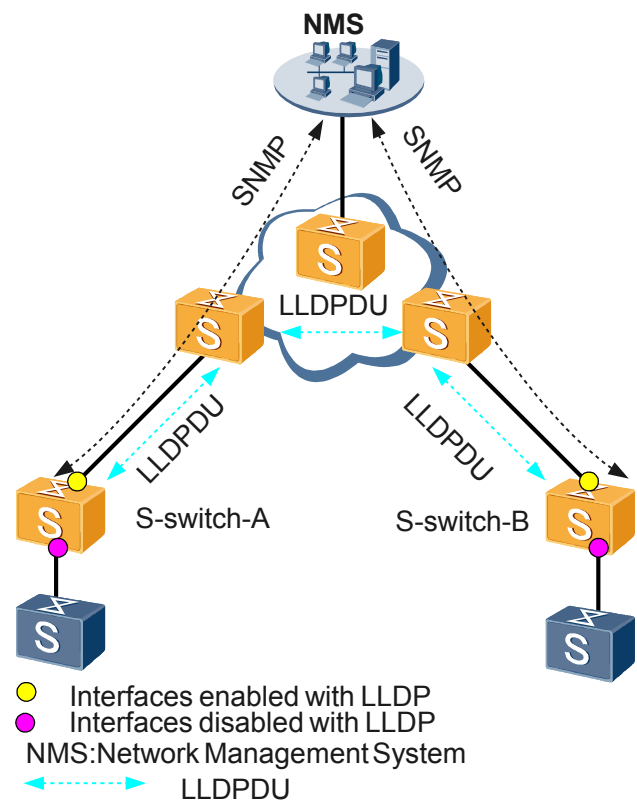
### 4.2.1 Establishing the Configuration Task

#### Applicable Environment

LLDP is used to obtain neighbor information and discover topologies. As shown in [Figure 4-1](#), when the NMS needs to collect the topology information on S-switch-A and S-switch-B, you can enable LLDP on S-switch-A and S-switch-B. In this manner, S-switch-A and S-switch-B can exchange their status information, thus, the NMS can obtain the topology information.

You need to set the LLDP management address on S-switch-A and S-switch-B so that the NMS can pinpoint S-switch-A and S-switch-B. You also need to enable the LLDP trap function on the S-switches so that the S-switches can send traps to the NMS when the network topology changes.

Figure 4-1 Networking diagram of LLDP application



Pre-configuration Tasks

Before configuring LLDP, complete the following tasks:

- Setting the IP address used as the LLDP management address

NOTE

The LLDP management address carried in an LLDP frame is used to identify a device. You need to select an IP address, for example, the IP address of the Management Ethernet (MEth) interface, so that the NMS can identify and manage easily. The IP address must be set before the LLDP management address is set.

Data Preparation

To configure LLDP, you need the following data.

| No. | Data                                                                               |
|-----|------------------------------------------------------------------------------------|
| 1   | IP address used as the LLDP management address                                     |
| 2   | Interval for sending LLDP frames                                                   |
| 3   | Delay for sending LLDP frames                                                      |
| 4   | Time multiplier of device information held in neighbor stations                    |
| 5   | Delay for the LLDP module on an interface to be re-enabled from the disabled state |

| No. | Data                                        |
|-----|---------------------------------------------|
| 6   | Delay for sending traps of neighbor changes |

## 4.2.2 (Optional) Enabling the LLDP Trap Function

### Context

Do as follows on S-switch-A and S-switch-B.

### Procedure

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

**Step 2** Run the **snmp-agent trap enable lldp** command to enable the LLDP trap function.

You need to enable the LLDP trap function on the S-switches so that the S-switches can send traps to the NMS when the network topology changes.



#### NOTE

When the LLDP trap function is enabled, the S-switch sends traps to the NMS when any of the following conditions is met:

- LLDP is disabled globally.
- The LLDP management address changes.
- Neighbor information changes. A trap is not generated if the management address of the neighbor changes.

----End

## 4.2.3 Enabling LLDP on an Interface

### Context

Do as follows on S-switch-A and S-switch-B.

### Procedure

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

**Step 2** Run the **lldp enable** command to enable LLDP globally.

**Step 3** Run the **bpdu enable** command to enable LLDP Bridge Protocol Data Units (BPDUs).

When the S-switch and its neighbors are all enabled with LLDP, the S-switch notifies the neighbors of its status and obtains the status of the neighbors by exchanging LLDP frames. The NMS can obtain information about Layer 2 connection status of the S-switch and then analyze the network topology.

----End

## 4.2.4 (Optional) Disabling LLDP on an Interface

### Context



#### NOTE

You can disable LLDP on an interface only after LLDP is enabled globally on the S-switch.

Do as follows on the interfaces that connect S-switch-A and S-switch-B to devices that need have LLDP disabled.

### 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 interface view.
- Step 3** Run the **undo lldp enable** command to disable LLDP on the interface.

When LLDP is enabled globally on the S-switch, all interfaces are enabled with LLDP by default. For the interfaces that do not require LLDP, you can run the **undo lldp enable** command in the interface view of these interfaces to disable LLDP.

----End

## 4.2.5 (Optional) Re-enabling LLDP on an Interface

### Context



#### NOTE

You can enable LLDP on an interface only when LLDP is enabled globally on the S-switch.

Do as follows on the interfaces that connect S-switch-A and S-switch-B to devices that need to be re-enabled with LLDP.

### 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 interface view.
- Step 3** Run the **lldp enable** command to re-enable LLDP on the interface.

When LLDP needs to be re-enabled on the interfaces where LLDP is disabled, you can run the **lldp enable** command in the interface view of these interfaces to re-enable LLDP.

----End

## 4.2.6 (Optional) Setting the LLDP Management Address

### Context



#### NOTE

You can set the LLDP management address only when LLDP is enabled globally on the S-switch.

Do as follows on S-switch-A and S-switch-B.

## Procedure

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

**Step 2** Run the **lldp management-address ip-address** command to set the LLDP management address.

The IP address must already exist on the S-switch. The IP address of the MEth interface is recommended as the LLDP management address.

----End

## 4.2.7 (Optional) Setting LLDP Attributes

### Context



#### NOTE

You can set LLDP attributes only when LLDP is enabled globally on the S-switch.

### (Optional) Setting the Interval for Sending LLDP Frames

### Prerequisite

Do as follows on S-switch-A and S-switch-B as required.

## Procedure

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

**Step 2** Run the **lldp message-transmission interval interval** command to set the interval for sending LLDP frames.

By default, the interval for sending LLDP frames is 30s.

The interval for sending LLDP frames must be set properly. You need to adjust the value of the parameter timely according to the network load.

- The greater the value, the lesser the frequency of LLDP frames being exchanged. This saves system resources. If the value is too great, that is, the delay for sending LLDP frames is too long, the S-switch cannot notify the neighbors of its status timely. As a result, the NMS cannot discover changes in the network topology timely. The smaller the value, the higher the frequency of the local status information being sent to the neighbors. This helps the NMS to discover changes in the network topology timely. If the value is too small, LLDP frames are exchanged too frequently. This increases the load on the system and wastes resources.

You must consider the value of *delay* when adjusting the value of *interval* because the two values affect each other.

- If the value of *interval* is not greater than 32768, you can add the value of *interval* regardless of the value of *delay*.
- If the value of *interval* is reduced, it must be not less than four times the value of *delay*. Thus, when the value of *interval* to be set is less than four times the value of *delay*, the value of

*delay* must be adjusted to be not greater than a quarter of the value of *interval*. After that, the value of *interval* can be set.

----End

## (Optional) Setting the Delay for Sending LLDP Frames

### Prerequisite

Do as follows on S-switch-A and S-switch-B as required.

### Procedure

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

**Step 2** Run the **lldp message-transmission delay** *delay* command to set the delay for sending LLDP frames.

The delay for sending LLDP frames must be set properly. You need to adjust the value of the parameter according to network load. The greater the value, the lesser the frequency of LLDP frames being exchanged. This saves system resources. If the value is too great, that is, the delay for sending LLDP frames is too long, the S-switch cannot notify the neighbors of its status timely. As a result, the NMS cannot discover changes in the network topology timely. The smaller the value, the higher the frequency of the local status information being sent to the neighbors. This helps the NMS to discover changes in the network topology timely. If the value is too small, however, LLDP frames are exchanged too frequently. This increases the load on the system and wastes resources.

By default, the value is 2s.

You must consider the value of *interval* when adjusting the value of *delay* because the two values affect each other.

- If the value of *delay* is not less than 1, you can decrease the value of *delay* regardless of the value of *interval*.
- If the value of *delay* is increased, it must be not greater than a quarter of the value of *interval*. Thus, when the value of *delay* to be set is greater than a quarter of the value of *interval*, the value of *interval* must be adjusted to be not less than four times the value of *delay*. After that, the value of *delay* can be set.

----End

## (Optional) Setting the Time Multiplier of Device Information Held in Neighbor Stations

### Prerequisite

Do as follows on S-switch-A and S-switch-B as required.

### Procedure

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

**Step 2** Run the **lldp message-transmission hold-multiplier** *hold* command to set the time multiplier of device information held in neighbor stations.

The greater the value is, the longer device information is held in the neighbor stations.

The default value is 4.

----End

## (Optional) Setting the Delay for Re-enabling LLDP on an Interface

### Prerequisite

Do as follows on S-switch-A and S-switch-B as required.

### Procedure

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

**Step 2** Run the **lldp restart-delay** *delay* command to set the delay for re-enabling LLDP on an interface.

When LLDP is disabled, you can re-enable LLDP on an interface after such a delay.

*delay* is set to control the status change of LLDP on an interface. This reduces the topology flapping of neighbor stations.

By default, the value is 2s.

----End

## (Optional) Setting the Delay for Sending Traps of Changes in Neighbor Information to the NMS

### Prerequisite

Do as follows on S-switch-A and S-switch-B as required.

### Procedure

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

**Step 2** Run the **lldp trap-interval** *interval* command to set the delay for sending traps of changes in neighbor information to the NMS.

When the neighbor information changes frequently, you can prolong the delay so that the S-switch sends traps to the NMS less frequently. This reduces the topology flapping.

The default value is 5s.

----End

## 4.2.8 Checking the Configuration

### Context

Run the following command to check the previous configuration.

| Action                                  | Command                                                                               |
|-----------------------------------------|---------------------------------------------------------------------------------------|
| Check the status of LLDP on the device. | <b>display lldp local</b> [ <b>interface</b> <i>interface-type interface-number</i> ] |

Run the **display lldp local** command. If the following information is displayed, it means that the configuration succeeds:

- LLDP is enabled on the S-switch.
- LLDP is enabled on the interfaces.
- The LLDP management address is 10.10.10.1.
- The LLDP trap function is disabled.
- The values for the following LLDP attributes are properly set:
  - Interval and delay for sending LLDP frames
  - Time multiplier of device information held in neighbors
  - Delay for re-enabling the LLDP module on an interface
  - Delay for sending traps of changes in neighbor information to the NMS

```
<Quidway> display lldp local
System information:
ChassisIdSubtype: macAddress
ChassisId: 0010-8300-0018
SysName:
Quidway
SysDesc: Quidway S3300 Series Ethernet Switches
Huawei Versatile Routing Platform Software
Copyright (C) 2005-2007 Huawei Technologies Co., Ltd.

SysCapSupported: bridge
SysCapEnabled: bridge
LLDPUpTime: 2008/1/9 1:17:39

System configuration:
LLDP enable status: enabled (default is disabled)
LldpMsgTxInterval: 30s (default is 30s)
LldpMsgTxHoldMultiplier: 4 (default is 4)
LldpReinitDelay: 2s (default is
2s)
LldpTxDelay: 2s (default is
2s)
LldpNotificationInterval: 5s (default is 5s)
LldpNotificationEnable: enabled (default is disabled)
Management address: IP: 192.168.32.23

Remote Table Statistics:
RemTablesLastChangeTime: 0 days, 0 hours, 0 minutes, 0 seconds
RemTableInserts: 0
RemTableDeletes: 0
RemTableDrops: 0
RemTablesAgeouts: 0
Neighbors Total: 0

Port information:
Interface Ethernet0/0/1:
PortId Subtype: interfaceName
PortId: Ethernet0/0/1
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/1 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0
```

```
Interface Ethernet0/0/2:
PortId Subtype: interfaceName
PortId: Ethernet0/0/2
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/2 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/3:
PortId Subtype: interfaceName
PortId: Ethernet0/0/3
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/3 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/4:
PortId Subtype: interfaceName
PortId: Ethernet0/0/4
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/4 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/5:
PortId Subtype: interfaceName
PortId: Ethernet0/0/5
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/5 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/6:
PortId Subtype: interfaceName
PortId: Ethernet0/0/6
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/6 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/7:
PortId Subtype: interfaceName
PortId: Ethernet0/0/7
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/7 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/8:
PortId Subtype: interfaceName
PortId: Ethernet0/0/8
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/8 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/9:
PortId Subtype: interfaceName
PortId: Ethernet0/0/9
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/9 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/10:
PortId Subtype: interfaceName
PortId: Ethernet0/0/10
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/10 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/11:
PortId Subtype: interfaceName
PortId: Ethernet0/0/11
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/11 Interface
LLDP Enable Status: enabled (default is disabled)
```

```
Neighbors Total: 0

Interface Ethernet0/0/12:
PortId Subtype: interfaceName
PortId: Ethernet0/0/12
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/12 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/13:
PortId Subtype: interfaceName
PortId: Ethernet0/0/13
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/13 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/14:
PortId Subtype: interfaceName
PortId: Ethernet0/0/14
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/14 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/15:
PortId Subtype: interfaceName
PortId: Ethernet0/0/15
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/15 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/16:
PortId Subtype: interfaceName
PortId: Ethernet0/0/16
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/16 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/17:
PortId Subtype: interfaceName
PortId: Ethernet0/0/17
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/17 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/18:
PortId Subtype: interfaceName
PortId: Ethernet0/0/18
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/18 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/19:
PortId Subtype: interfaceName
PortId: Ethernet0/0/19
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/19 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/20:
PortId Subtype: interfaceName
PortId: Ethernet0/0/20
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/20 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/21:
PortId Subtype: interfaceName
PortId: Ethernet0/0/21
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/21 Interface
```

```

LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/22:
PortId Subtype: interfaceName
PortId: Ethernet0/0/22
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/22 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/23:
PortId Subtype: interfaceName
PortId: Ethernet0/0/23
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/23 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface Ethernet0/0/24:
PortId Subtype: interfaceName
PortId: Ethernet0/0/24
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/24 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface GigabitEthernet0/0/1:
PortId Subtype: interfaceName
PortId: GigabitEthernet0/0/1
PortDesc: HUAWEI, Quidway Series, GigabitEthernet0/0/1 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

Interface GigabitEthernet0/0/2:
PortId Subtype: interfaceName
PortId: GigabitEthernet0/0/2
PortDesc: HUAWEI, Quidway Series, GigabitEthernet0/0/2 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0

```

## 4.3 Maintaining LLDP

This section describes how to maintain and debug LLDP.

### 4.3.1 Clearing the LLDP Statistics

#### 4.3.2 Monitoring the Running Status of LLDP

### 4.3.1 Clearing the LLDP Statistics

#### Context

To clear the statistics on LLDP frames, run the **reset lldp statistic** command in the user view.

| Action                                                                                                                                                                | Command                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Clear the statistics on LLDP frames on an interface. The statistics include the number of received frames, the number of sent frames, and the number of error frames. | <b>reset lldp statistic</b> [ <b>interface</b> <i>interface-type interface-number</i> ] |

## 4.3.2 Monitoring the Running Status of LLDP

### Context

To check the running status of LLDP during routine maintenance, run the following **display** commands in the user view.

| Action                                                                 | Command                                                                                    |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Check the LLDP status globally or on a specified interface.            | <b>display lldp local</b> [ <b>interface</b> <i>interface-type interface-number</i> ]      |
| Check the statistics on LLDP frames sent and received on an interface. | <b>display lldp statistics</b> [ <b>interface</b> <i>interface-type interface-number</i> ] |
| Check the neighbor information on an interface.                        | <b>display lldp neighbor</b> [ <b>interface</b> <i>interface-type interface-number</i> ]   |

## 4.4 Configuration Examples

This section provides several configuration examples of LLDP.

### [4.4.1 Example for Configuring LLDP](#)

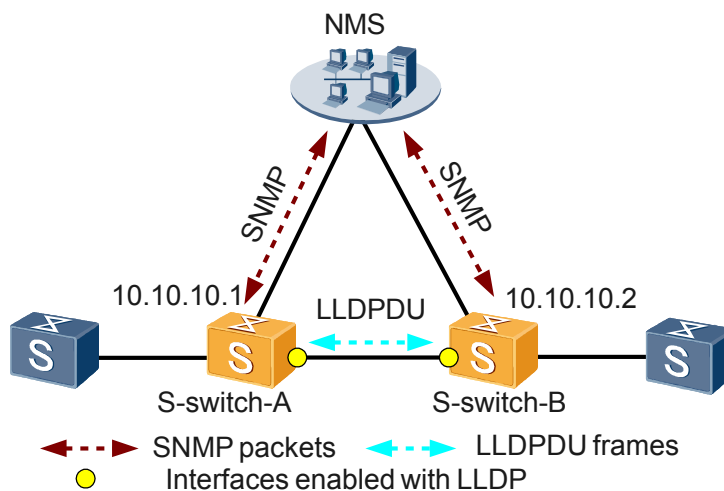
#### [4.4.2 Example for Configuring LLDP on the Network an Eth-Trunk](#)

### 4.4.1 Example for Configuring LLDP

#### Context

#### Networking Requirements

As shown in [Figure 4-2](#), S-switch-A and S-switch-B are directly connected through Ethernet interfaces. There are routes between S-switch-A and the NMS and between S-switch-B and the NMS. It is required that S-switch-A and S-switch-B should obtain the status of each other through the LLDP protocol, and the NMS should locate S-switch-A and S-switch-B based on the LLDP management address to discover the topology. When the LLDP management address changes, LLDP is disabled globally, or neighbor information changes, S-switch-A and S-switch-B should send LLDP traps to the NMS.

**Figure 4-2** Networking for configuring LLDP

## Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the LLDP trap function on S-switch-A and S-switch-B.
2. Enable LLDP globally on S-switch-A and S-switch-B.
3. Enable the S-switch-A and S-switch-B to process LLDP BPDUs.
4. Set a management address for S-switch-A and S-switch-B respectively.
5. Set LLDP attributes for S-switch-A and S-switch-B.

## Data Preparation

To complete the configuration, you need the following data:

- The management address of S-switch-A is 10.10.10.1, and the management address of S-switch-B is 10.10.10.2.
- Ethernet 0/0/1 on S-switch-A and S-switch-B respectively is enabled with LLDP.
- The interval for sending LLDP frames is 60 seconds. The delay for sending LLDP frames is 9 seconds. The delay for sending traps of changes in neighbor information to the NMS is 10 seconds.

## Configuration Procedure

1. Enable the LLDP trap function on S-switch-A and S-switch-B.

# Configure S-switch-A.

```
<Quidway> system-view
[Quidway] sysname S-switch-A
[S-switch-A] snmp-agent trap enable lldp
```

# Configure S-switch-B.

```
<Quidway> system-view
[Quidway] sysname S-switch-B
[S-switch-B] snmp-agent trap enable lldp
```

2. Enable LLDP globally on S-switch-A and S-switch-B.

# Configure S-switch-A.

- ```
[S-switch-A] lldp enable
```
- # Configure S-switch-B.
- ```
[S-switch-B] lldp enable
```
3. Enable the S-switch-A and S-switch-B to process LLDP BPDUs.  
# Configure S-switch-A.  

```
[S-switch-A] bpdu enable
```

  
# Configure S-switch-B.  

```
[S-switch-B] bpdu enable
```
  4. Set a management address for S-switch-A and S-switch-B respectively.  
# Configure S-switch-A.  

```
[S-switch-A] lldp management-address 10.10.10.1
```

  
# Configure S-switch-B.  

```
[S-switch-B] lldp management-address 10.10.10.2
```
  5. Set LLDP attributes for S-switch-A and S-switch-B.  
# Configure S-switch-A.  

```
[S-switch-A] lldp message-transmission interval 60
[S-switch-A] lldp message-transmission delay 9
[S-switch-A] lldp trap-interval 10
```

  
# Configure S-switch-B.  
See the configuration of S-switch-A.
  6. Verify the configuration.  
# Check whether LLDP is enabled, whether the LLDP management address is set, whether the LLDP trap function is enabled, and whether the values of LLDP attributes are properly set.
    - Check the configuration on S-switch-A.  

```
[S-switch-A] display lldp local
```

System information:  
ChassisIdSubtype: macAddress  
ChassisId: 0200-0000-0000  
SysName: S-switch-A  
Huawei Versatile Routing Platform Software  
Copyright (C) 2005-2007 Huawei Technologies Co., Ltd.  
SysCapSupported: bridge  
SysCapEnabled: bridge  
LLDPUpTime: 2008/1/1 0:1:36  
System configuration:  
LLDP enable status: enabled (default is disabled)  
LldpMsgTxInterval: 60s (default is 30s)  
LldpMsgTxHoldMultiplier: 4 (default is 4)  
LldpReinitDelay: 2s (default is 2s)  
LldpTxDelay: 9s (default is 2s)  
LldpNotificationInterval: 10s (default is 5s)  
LldpNotificationEnable: enabled (default is disabled)  
Management address: IP: 10.10.10.1  
Remote Table Statistics:  
RemTablesLastChangeTime: 1 days, 4 hours, 19 minutes, 55 seconds  
RemTableInserts: 4  
RemTableDeletes: 4  
RemTableDrops: 0  
RemTablesAgeouts: 0  
Neighbors Total: 1  
  
Port  
information:  
Interface  
Ethernet0/0/1:

```
PortId Subtype:
interfaceName
PortId:
Ethernet0/0/1
PortDesc: Huawei, Quidway Series, Ethernet0/0/1
Interface
LLDP Enable Status: enabled (default is
disabled)
Neighbors Total: 0
```

- Check the configuration on S-switch-B.  
For details, see the configuration on S-switch-A.

## Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
lldp enable
bpdu enable
#
snmp-agent trap enable lldp
#
lldp message-transmission interval 60
#
lldp message-transmission delay 9
#
lldp trap-interval 10
#
lldp management-address 10.10.10.1
#
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
lldp enable
bpdu enable
#
snmp-agent trap enable lldp
#
lldp message-transmission interval 60
#
lldp message-transmission delay 9
#
lldp trap-interval 10
#
lldp management-address 10.10.10.2
#
return
```

### 4.4.2 Example for Configuring LLDP on the Network an Eth-Trunk

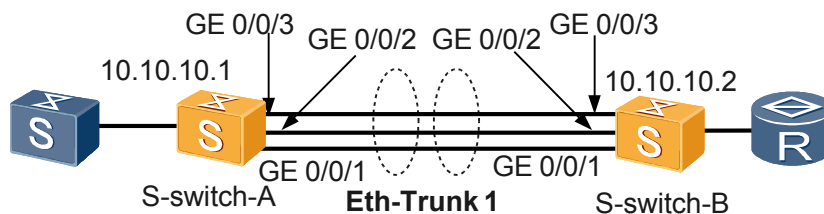
#### Context

#### Networking Requirements

As shown in [Figure 4-3](#), S-switch-A and S-switch-B are connected through an Eth-Trunk. It is required that three Ethernet interfaces on S-switch-A and S-switch-B respectively be added to the Eth-Trunk. In addition, two of the three Ethernet interfaces on S-switch-A and S-switch-B respectively should send and receive LLDP frames to obtain the status of each other. The other

Ethernet interface on S-switch-A and S-switch-B respectively is disabled to send or receive LLDP frames.

**Figure 4-3** Networking for configuring LLDP on the network with an Eth-Trunk



## Configuration Roadmap

The configuration roadmap is as follows:

1. Enable LLDP globally on S-switch-A and S-switch-B.
2. Set a management address for S-switch-A and S-switch-B respectively so that the NMS can identify the devices.
3. Add Ethernet interfaces on S-switch-A and S-switch-B to an Eth-Trunk.
4. Disable LLDP on the member interfaces on S-switch-A and S-switch-B that are added to the Eth-Trunk.
5. Configure the S-switch-A and S-switch-B to process LLDP BPDUs.

## Data Preparation

To complete the configuration, you need the following data:

- The management address of S-switch-A is 10.10.10.1, and the management address of S-switch-B is 10.10.10.2.
- The number of the Eth-Trunk that connects S-switch-A and S-switch-B, and the numbers of the interfaces that are added to the Eth-Trunk

## Configuration Procedure

1. Enable LLDP globally on S-switch-A and S-switch-B.

# Configure S-switch-A.

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

# Configure S-switch-B.

See the configuration of S-switch-A.

2. Set a management address for S-switch-A and S-switch-B respectively so that the NMS can identify the devices.

# Configure S-switch-A.

```
[S-switch-A] lldp management-address 10.10.10.1
```

# Configure S-switch-B.

```
[S-switch-B] lldp management-address 10.10.10.2
```

3. Configure an Eth-Trunk on S-switch-A and S-switch-B.

# Configure S-switch-A.

```
[S-switch-A] interface eth-trunk 1
[S-switch-A-Eth-Trunk1] quit
[S-switch-A] interface ethernet 0/0/1
[S-switch-A-Ethernet0/0/1] eth-trunk 1
[S-switch-A-Ethernet0/0/1] quit
[S-switch-A] interface ethernet 0/0/2
[S-switch-A-Ethernet0/0/2] eth-trunk 1
[S-switch-A-Ethernet0/0/2] quit
[S-switch-A] interface ethernet 0/0/3
[S-switch-A-Ethernet0/0/3] eth-trunk 1
```

#### # Configure S-switch-B.

```
[S-switch-B] interface eth-trunk 1
[S-switch-B-Eth-Trunk1] quit
[S-switch-B] interface ethernet 0/0/1
[S-switch-B-Ethernet0/0/1] eth-trunk 1
[S-switch-B-Ethernet0/0/1] quit
[S-switch-B] interface ethernet 0/0/2
[S-switch-B-Ethernet0/0/2] eth-trunk 1
[S-switch-B-Ethernet0/0/2] quit
[S-switch-B] interface ethernet 0/0/3
[S-switch-B-Ethernet0/0/3] eth-trunk 1
```

4. Disable LLDP on the member interfaces on S-switch-A and S-switch-B that are added to the Eth-Trunk.

#### # Configure S-switch-A.

```
[S-switch-A-Ethernet0/0/3] undo lldp enable
[S-switch-A-Ethernet0/0/3] quit
```

#### # Configure S-switch-B.

```
[S-switch-B-Ethernet0/0/3] undo lldp enable
[S-switch-B-Ethernet0/0/3] quit
```

5. Configure the S-switch-A and S-switch-B to process LLDP BPDUs.

#### # Configure S-switch-A.

```
[S-switch-A] bpdud enable
```

#### # Configure S-switch-B.

```
[S-switch-B] bpdud enable
```

6. Verify the configuration.

# Check whether LLDP is enabled, whether the LLDP management address is set, and whether the LLDP status on the member interfaces of Eth-Trunk 1 is displayed as configured.

#### ● Check the configuration on S-switch-A.

```
[S-switch-A] display lldp local
System information:
ChassisIdSubtype: macAddress
ChassisId: 0200-0000-0000
SysName: S-switch-A
Huawei Versatile Routing Platform Software
Copyright (C) 2005-2007 Huawei Technologies Co., Ltd.
```

```
SysCapSupported: bridge
SysCapEnabled: bridge
LLDPUpTime: 2008/1/1 0:1:36
```

```
System configuration:
LLDP enable status: enabled (default is disabled)
LldpMsgTxInterval: 30s (default is 30s)
LldpMsgTxHoldMultiplier: 4 (default is 4)
LldpReinitDelay: 2s (default is 2s)
LldpTxDelay: 2s (default is 2s)
LldpNotificationInterval: 5s (default is 5s)
LldpNotificationEnable: disabled (default is disabled)
```

```

Management address: IP: 10.10.10.1
Remote Table Statistics:
RemTablesLastChangeTime: 2 days, 3 hours, 59 minutes, 54 seconds
RemTableInserts: 5
RemTableDeletes: 4
RemTableDrops: 0
RemTablesAgeouts: 0
Neighbors Total: 2
Port information:
Interface Ethernet0/0/1:
PortId Subtype: interfaceName
PortId: Ethernet0/0/1
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/1 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0
Interface Ethernet0/0/2:
PortId Subtype: interfaceName
PortId: Ethernet0/0/2
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/2 Interface
LLDP Enable Status: enabled (default is disabled)
Neighbors Total: 0
Interface Ethernet0/0/3:
PortId Subtype: interfaceName
PortId: Ethernet0/0/3
PortDesc: HUAWEI, Quidway Series, Ethernet0/0/3 Interface
LLDP Enable Status: disabled (default is disabled)
Neighbors Total: 0

```

- Check the configuration on S-switch-B.

For details, see the configuration on S-switch-A.

# Check whether the member interfaces are added to Eth-Trunk 1.

- Check the configuration on S-switch-A.

```

[S-switch-A] display trunkmembership eth-trunk 1
Trunk ID: 1
used status: VALID
TYPE: ethernet
Number Of Ports in Trunk = 3
Number Of UP Ports in Trunk = 3
operate status: up
Interface Ethernet0/0/1, valid,selected,operate up,weight=1,standby interface
NULL
Interface Ethernet0/0/2, valid,selected,operate up,weight=1,standby interface
NULL
Interface Ethernet0/0/3, valid,selected,operate up,weight=1,standby interface
NULL

```

- Check the configuration on S-switch-B.

For details, see the configuration on S-switch-A.

## Configuration Files

- Configuration file of S-switch-A

```

#
 sysname S-switch-A
#
 lldp enable
 bpdu enable
#
 interface Eth-Trunk1
#
 interface Ethernet0/0/1
 eth-trunk 1
#
 interface Ethernet0/0/2
 eth-trunk 1

```

```
#
interface Ethernet0/0/3
 eth-trunk 1
 undo lldp enable
#
 lldp management-address 10.10.10.1
#
return
```

- Configuration file of S-switch-B

```
#
 sysname S-switch-B
#
 lldp enable
 bpdu enable
#
interface Eth-Trunk1
#
interface Ethernet0/0/1
 eth-trunk 1
#
interface Ethernet0/0/2
 eth-trunk 1
#
interface Ethernet0/0/3
 eth-trunk 1
 undo lldp enable
#
 lldp management-address 10.10.10.2
#
return
```

# 5 NQA Configuration

---

## About This Chapter

This chapter describes the basic principle of Network Quality Analysis (NQA), compares NQA with the **ping** command, describes multiple tests, describes common parameters, and provides configuration examples.

### Context

#### [5.1 Introduction](#)

This section describes basic concepts and functions of NQA.

#### [5.2 Configuring an ICMP Test](#)

This section describes how to perform an ICMP test by using NQA.

#### [5.3 Configuring a DHCP Test](#)

This section describes how to test the speed at which a DHCP client sets up a connection with a DHCP server for obtaining an IP address.

#### [5.4 Configuring the FTP Download Test](#)

This section describes how to test the performance of the File Transfer Protocol (FTP) download function.

#### [5.5 Configuring an FTP Upload Test](#)

This section describes how to test the performance of the FTP upload function.

#### [5.6 Configuring an HTTP Test](#)

This section describes how to test the response speed of the HTTP service in each phase.

#### [5.7 Configuring the SNMP Query Test](#)

This section describes how to test the status of the communication between hosts and SNMP agents.

#### [5.8 Configuring a TCP Test](#)

This section describes how to test the response speed of the TCP interface.

#### [5.9 Configuring a UDP Test](#)

This section describes how to test the response speed of the UDP port.

#### [5.10 Configuring a Jitter Test](#)

This section describes how to test the jitter of processing UDP packets.

#### [5.11 Configuring an NQA Test Group](#)

This section describes how to configure an NQA test group.

#### [5.12 Configuring Universal NQA Test Parameters](#)

This section describes how to configure universal parameters for NQA tests.

#### [5.13 Configuring the Bidirectional Transmission Delay Threshold](#)

This section describes how to configure the bidirectional transmission delay threshold for an NQA test.

#### [5.14 Configuring the Unidirectional Transmission Delay Threshold](#)

This section describes how to configure the unidirectional transmission delay threshold for an NQA test.

#### [5.15 Configuring the Trap Function](#)

This section describes how to configure the trap function in an NQA test.

#### [5.16 Maintaining NQA](#)

This section describes how to maintain NQA.

#### [5.17 Configuration Examples](#)

This section provides several configuration examples of NQA.

## 5.1 Introduction

This section describes basic concepts and functions of NQA.

### 5.1.1 Overview of NQA

#### 5.1.2 Comparisons Between NQA and Ping

#### 5.1.3 NQA Client and NQA Server

#### 5.1.4 NQA Features Supported by the S-switch

### 5.1.1 Overview of NQA

As the development of value-added services, users and carriers demand higher Quality of Service (QoS). After voice over IP and video over IP services are carried out, carriers and users all tend to sign Service Level Agreements (SLAs) to realize QoS guaranteed services.

To help users know the performance of the network in time, carriers should collect statistics of delay, jitter, and packet loss ratio of the device. In this case, users can check whether the committed bandwidth is ensured.

NQA on the S-switch can meet the preceding requirements.

NQA tests the performance of different protocols running on the network. In that case, carriers can collect the operation index of networks in real time, such as total delay of the Hypertext Transfer Protocol (HTTP), delay in the Transmission Control Protocol (TCP) connection, file transmission speed, and delay in File Transfer Protocol (FTP) connection. Taking control of these indexes, carriers can provide network services of different levels and charge differently.

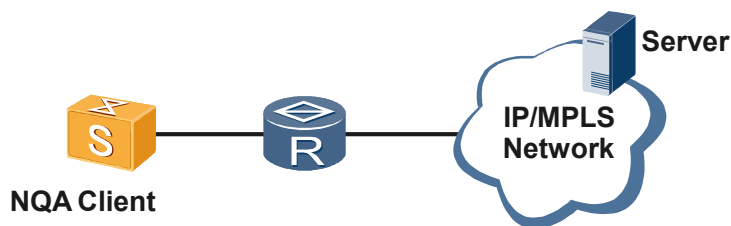
NQA is also an effective tool for diagnosing and locating faults over a network.

### 5.1.2 Comparisons Between NQA and Ping

NQA is an extension and enhancement of ping.

Using the Internet Control Message Protocol (ICMP), the ping tool tests the round-trip time (RTT) of a packet to travel between the current interface and the destination interface. NQA can also test the RTT of a packet. In addition, NQA can detect whether the Transmission Control Protocol (TCP), the User Datagram Protocol (UDP), the Dynamic Host Configuration Protocol (DHCP), the File Transfer Protocol (FTP), or the Hypertext Transfer Protocol (HTTP) are enabled, and test the response time of services. **Figure 5-1** shows how NQA functions.

**Figure 5-1** Diagram of an NQA test



Different from the ping tool that displays in real time the RTT of a packet or whether a packet times out on the console interface, NQA displays the result of the test through the **display nqa results** command after a test is complete.

You can set parameters for each NQA operation through the Network Management System (NMS) and then perform the NQA test.

### 5.1.3 NQA Client and NQA Server

#### NQA Test and NQA Client

NQA can test many items. You must create a test instance for each item, and each test instance is a type of NQA tests.

NQA test instances are created on NQA clients. Each test instance has an administrator name and an operation tag, which can uniquely identify a test instance.

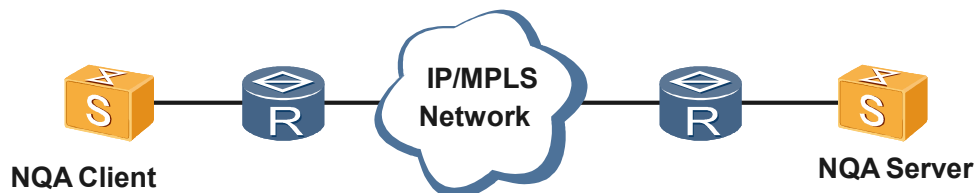
In the test instance view, the related test parameters are configured. Some parameters are valid only for some types of tests whereas some are valid for all tests.

#### NQA Server

In most types of tests, only NQA clients need to be configured. The NQA server, however, must be configured in tests concerning TCP, UDP, and jitter.

The NQA server processes the test packets received from the NQA client. As shown in [Figure 5-2](#), the NQA server responds to the test initiated by the client through the monitoring function.

**Figure 5-2** Relationships between the NQA client and the NQA server



You can create multiple TCP or UDP monitoring services on an NQA server. Each monitoring service involves a set of specified destination addresses and interface numbers. The destination addresses and interface numbers can be repeatedly specified.

#### Performing NQA Tests

The NQA server can respond to the test request sent by the client only after being configured with the monitoring addresses and interface numbers. The IP address and interface number specified in the monitoring service must be the same as those configured on the client.

After creating the test instance and the configuring related parameters, you can start the NQA test by running the **start** command and view test results by running the **display nqa results** command.

### 5.1.4 NQA Features Supported by the S-switch

## Features Provided by NQA

- Cooperates with the NMS:  
Manages all NQA functions completely.  
Supports the NQA Management Information Base (MIB) user interface.
- Supports multiple types of tests:  
ICMP test  
DHCP test  
FTP test  
HTTP test  
SNMP test  
DNS test  
TCP test  
UDP test  
UDP jitter test
- In jitter tests, up to 3000 packets can be sent continuously and voice traffic can be simulated.
- Supports 2000 tests.
- Supports statistics at the millisecond level.
- Supports the task scheduling of tests.  
Implements the scheduling of the test to reduce the burden caused by concurrent tasks on a device.  
Supports the configuration of different start time and end time for a single test.
  - Supports three modes of starting tests: immediate, delayed, and at a fixed time.
  - Supports five modes of ending tests: automatic, immediate, delayed, at a fixed time, and ending tests when the life cycle of the test expires.When several tasks are performed at the same time, the device reasonably arranges start time and test intervals.
- Supports the configuration of test groups for managing only the ICMP and jitter tests.
- Supports the auto-delay function. This function can make full use of system resources to complete the tests within the specified period.
- Supports unidirectional and bidirectional delay statistics. In addition, you can set a threshold and collect statistics on packets that exceed the threshold.
- Supports unidirectional packet loss statistics.

## NQA Restriction

At present, NQA supports only IPv4 addresses.

## 5.2 Configuring an ICMP Test

This section describes how to perform an ICMP test by using NQA.

### Context

[5.2.1 Establishing the Configuration Task](#)[5.2.2 Configuring ICMP Test Parameters](#)[5.2.3 Checking the Configuration](#)

## 5.2.1 Establishing the Configuration Task

### Applicable Environment

The ICMP test has a similar function with the **ping** command. It provides more output.

### Pre-configuration Tasks

Before configuring the ICMP test, configure reachable routes between the NQA client and the tested device.

### Data Preparation

To configure the ICMP test, you need the following data.

| No. | Data                                                                                                                                                                                                                                                                                              |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Administrator name and test name                                                                                                                                                                                                                                                                  |
| 2   | Destination IP address                                                                                                                                                                                                                                                                            |
| 3   | (Optional) Virtual Private Network (VPN) instance name, source interface that sends test packets, source IP address, size of the Echo Request packets, Time to Live (TTL) value, Type of Service (ToS), pad characters, interval for sending test packets, and percentage of the failed NQA tests |
| 4   | Start mode and end mode                                                                                                                                                                                                                                                                           |

## 5.2.2 Configuring ICMP Test Parameters

### Context

Do as follows on the NQA client.

### Procedure

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

**Step 2** Run the **nqa test-instance** *admin-name test-name* command to establish an NQA test and enter the test interface view.

**Step 3** Run the **test-type icmp** command to configure an ICMP test.

NQA tests default to ICMP tests.

**Step 4** Run the **destination-address ipv4** *ip-address* command to configure the destination IP address.

**Step 5** (Optional) Run the following commands to configure other parameters for the ICMP test.

- Run the **vpn-instance** *vpn-instance-name* command to configure a VPN test instance.
- Run the **source-interface** [ *interface-type interface-number* ] command to configure the source interface for sending test packets.
- Run the **source-address ipv4** *ip-address* command to configure the source IP address. This parameter functions the same as the **-a** option in the **ping** command.  
If the destination IP address and the source IP address are in different network segments, you cannot use this command. Otherwise, NQA tests fail.
- Run the **datasize** *size* command to set the size of Echo Request packets excluding the IP header. This parameter functions the same as the **-s** option in the **ping** command.
- Run the **ttl** *value* command to set the TTL value. This parameter functions the same as the **-h** option in the **ping** command.
- Run the **tos** *value* command to configure the service type specified by the value of the ToS field in an IP header. This parameter functions the same as the **-tos** option in the **ping** command.
- Run the **datafill** *string* command to configure the pad character. This parameter functions the same as the **-p** option in the **ping** command.
- Run the **interval seconds** *interval* command to set the interval for sending test packets. This parameter functions the same as the **-m** option in the **ping** command.
- Run the **fail-percent** *percent* command to configure the percentage of the failed NQA tests.
- Run the **sendpacket passroute** command to configure that the NQA test packets are sent without searching the routing table.

**Step 6** Run the **start** command to start the NQA test.

The **start** command has several forms. You can choose one of the following forms as required:

- Run the **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start the test immediately.
- Run the **start at** [ *yyyy/mm/dd* ] *hh:mm:ss* [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start a test at a fixed time.
- Run the **start delay** { **seconds** *second* | *hh:mm:ss* } [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start a test at a delayed time.

----End

## 5.2.3 Checking the Configuration

### Context

Run the following commands to check the previous configuration.

| Action                                                                     | Command                                                    |
|----------------------------------------------------------------------------|------------------------------------------------------------|
| Check the test results on the NQA client.                                  | <b>display nqa results</b> [ <i>admin-name test-name</i> ] |
| Check information about the task scheduling of the test on the NQA client. | <b>display nqa-schedule</b>                                |

NQA test results cannot be displayed automatically on the terminal. You can run the **display nqa results** command to check the results of the latest five tests.

Run the **display nqa results** command. If the following information is displayed, it means that the test succeeds.

- testFlag is inactive
- The test is finished
- Completion:success

You can also view the minimum time, the maximum time, and the average time of receiving the response packet when an ICMP NQA test is configured.

```
<Quidway> display nqa results
NQA entry(admin, icmp) :testFlag is inactive ,testtype is icmp
1 . Test 1 result The test is finished
 Send operation times :3 Receive response times :3
 Completion :success RTD OverThresholds number:0
 Attempts number :1 Drop operation number :0
 Disconnect operation number :0 Operation timeout number :0
 System busy operation number :0 Connection fail number :0
 Operation sequence errors number:0 RTT Stats errors number :0
 Destination ip address :10.1.1.2
 Min/Max/Average Completion Time :1/1/1
 Sum/Square-Sum Completion Time :3/3
 Last Good Probe Time: 2008-1-1 0:21:35.3
```

Run the **display nqa-schedule** command to check information about the task scheduling of the current NQA test.

```
<Quidway> display nqa-schedule
NQA Tests Max:2000 NQA Tests Num:1
NQA Concurrent Requests Max:1000 NQA Concurrent Requests Num:0
NQA Jitter Concurrent Max:5 NQA Jitter Concurrent Num:0
NQA icmp Concurrent Max:50 NQA icmp Concurrent Num:0
NQA Trace Concurrent Max:50 NQA Trace Concurrent Num:0
Index Schedule Time Type nqa icmp jitter packets
1 start 2007-11-19 8:44:20 icmp 1 1 0 0
2 end 2007-11-19 8:44:31 icmp 0 0 0 0
```

## 5.3 Configuring a DHCP Test

This section describes how to test the speed at which a DHCP client sets up a connection with a DHCP server for obtaining an IP address.

### Context

#### 5.3.1 Establishing the Configuration Task

### [5.3.2 Configuring DHCP Test Parameters](#)

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

## 5.3.1 Establishing the Configuration Task

### Applicable Environment

Through the DHCP test, you can obtain the following information:

- Time for a client to set up a connection with a DHCP server
- Time for a client to obtain its IP address

### Pre-configuration Tasks

Before configuring the DHCP test, complete the following tasks:

- Configuring the DHCP server or the DHCP relay agent
- Configuring the routes between the NQA client and the DHCP server or between the NQA client and the DHCP relay agent

### Data Preparation

To configure the DHCP test, you need the following data.

| No. | Data                                                                                 |
|-----|--------------------------------------------------------------------------------------|
| 1   | Administrator name and test name                                                     |
| 2   | Outbound interface connected to the DHCP server                                      |
| 3   | (Optional) Timeout period of the test packets and percentage of the failed NQA tests |
| 4   | Start mode and end mode of the test                                                  |

## 5.3.2 Configuring DHCP Test Parameters

### Context

Do as follows on the NQA client.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.
- Step 3** Run the **test-type dhcp** command to configure a DHCP test.

- Step 4** Run the **source-interface** *interface-type interface-number* command to specify the source interface for sending DHCP request packets.

The source interface can be an Ethernet interface connected with the DHCP server, an Eth-Trunk interface, or a VLANIF interface.

- Step 5** (Optional) Run the following commands to configure other parameters for the DHCP test.

- Run the **timeout** *time* command to set the timeout period for the NQA test.

 **NOTE**

For the DHCP test, the time taken to wait for the response to the packet may reach 10 seconds. By default, the timeout period is 15 seconds. It is recommended that you set the timeout period longer than 10 seconds.

- Run the **fail-percent** *percent* command to set the percentage of the failed NQA tests.

- Step 6** Run the **start** command to start the NQA test.

The **start** command has several forms. You can choose one of the following forms as required:

- Run the **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start the test immediately.
- Run the **start at** [ *yyyy/mm/dd* ] *hh:mm:ss* [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start the test at a fixed time.
- Run the **start delay** { **seconds** *second* | *hh:mm:ss* } [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start the test at a delayed time.

----End

## 5.3.3 Checking the Configuration

### Context

Run the following commands to check the previous configuration.

| Action                                                                     | Command                                                    |
|----------------------------------------------------------------------------|------------------------------------------------------------|
| Check the test results on the NQA client.                                  | <b>display nqa results</b> [ <i>admin-name test-name</i> ] |
| Check information about the task scheduling of the test on the NQA client. | <b>display nqa-schedule</b>                                |

NQA test results cannot be displayed automatically on the terminal. You can run the **display nqa results** command to check the test results for the recent five times.

Run the **display nqa results** command. If the following information is displayed, it means that the test succeeds.

- testFlag is inactive

- The test is finished
- Completion:success

For the DHCP test, you can also view the following information in the extended results:

- Number of times to disconnect with the server and times of the disconnection timeout
- Number of times that the server becomes busy and number of times of the failed disconnections
- Number of times of incorrect operation sequences and number of times of the discarding operations
- Number of times of incorrect operations for collecting statistics

```
<Quidway> display nqa results
NQA entry(admin, dhcp) :testFlag is inactive ,testtype is dhcp
1 . Test 1 result The test is finished
 Send operation times: 3 Receive response times: 2
 Completion:success RTD OverThresholds number: 0
 Attempts number:1 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:2
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:10.1.1.3
 Min/Max/Average Completion Time: 1030/1030/1030
 Sum/Square-Sum Completion Time: 1030/1060900
 Last Good Probe Time: 2007-6-29 16:00:22
```

Run the **display nqa-schedule** command to check information about the task scheduling of the current NQA test.

```
<Quidway> display nqa-schedule
NQA Tests Max:2000 NQA Tests Num:1
NQA Concurrent Requests Max:1000 NQA Concurrent Requests Num:0
NQA Jitter Concurrent Max:5 NQA Jitter Concurrent Num:0
NQA icmp Concurrent Max:50 NQA icmp Concurrent Num:0
NQA Trace Concurrent Max:50 NQA Trace Concurrent Num:0
Index Schedule Time Type nqa icmp jitter packets
1 start 2007-11-19 8:56:18 dhcp 1 0 0 0
2 end 2007-11-19 8:57:3 dhcp 0 0 0 0
```

## 5.4 Configuring the FTP Download Test

This section describes how to test the performance of the File Transfer Protocol (FTP) download function.

### Context

#### 5.4.1 Establishing Configuration Tasks

#### 5.4.2 Configuring the FTP Download Test Parameters

#### 5.4.3 Checking the Configuration

### 5.4.1 Establishing Configuration Tasks

#### Applicable Environment

In the FTP download test, the local device functions as an FTP client to download the specified file from the FTP server.

Statistics about each FTP phase are displayed, including the time to set up FTP control connection and the time to transport the data.

## Pre-configuration Tasks

Before configuring the FTP download test, complete the following tasks:

- Configuring the FTP user name, password, and the login directory
- Configuring that the NQA client and the FTP server are reachable

## Data Preparation

To configure the FTP download test, you need the following data.

| No. | Data                                                                                           |
|-----|------------------------------------------------------------------------------------------------|
| 1   | Administrator name and test name                                                               |
| 2   | IP address of the FTP server                                                                   |
| 3   | The source IP address of the FTP operation                                                     |
| 4   | (Optional) VPN instance name and source and destination interface numbers of the FTP operation |
| 5   | FTP user name and password                                                                     |
| 6   | Name of the file to be downloaded                                                              |
| 7   | Start mode and end mode of the test                                                            |

## 5.4.2 Configuring the FTP Download Test Parameters

### Context

Do as follows on the NQA client that also functions as the FTP client.

### Procedure

- Step 1** Run the **system-view?** command to enter the system view.
- Step 2** Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.
- Step 3** Run the **test-type ftp** command to configure an FTP test.
- Step 4** Run the **destination-address ipv4** *ip-address* command to configure the destination IP address.
- Step 5** Run the **source-address ipv4** *ip-address* command to configure the source IP address.
- Step 6** (Optional) Run the following commands to configure other parameters for the FTP test.
- Run the **vpn-instance** *vpn-instance-name* command to configure a VPN test instance.

- Run the **source-port** *port-number* command to configure the source interface number.
- Run the **destination-port** *port-number* command to configure the destination interface number.
- Run the **sendpacket passroute** command to configure that the NQA test packets are sent without searching the routing table.

**Step 7** Run the **ftp-operation get** command to set the FTP operation type to **get**.

By default, the FTP operation type is **get**.

**Step 8** Run the **ftp-username** *name* command to configure the FTP user name.

**Step 9** Run the **ftp-password** *password* command to configure the FTP password.

**Step 10** Run the **ftp-filename** *file-name* command to configure the name of the file that is to be downloaded.



**NOTE**

During the FTP test, select a file of relatively small size. If the file is too large, the test may fail because of timeout.

**Step 11** Run the **start** command to start the NQA test.

The **start** command has several forms. You can choose one of the following forms as required:

- Run the **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start the test immediately.
- Run the **start at** [ *yyyy/mm/dd* ] *hh:mm:ss* [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start the test at a fixed time.
- Run the **start delay** { **seconds** *second* | *hh:mm:ss* } [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start the test at a delayed time.

----End

## 5.4.3 Checking the Configuration

### Context

Run the following commands to check the previous configuration.

| Action                                                                     | Command                                                    |
|----------------------------------------------------------------------------|------------------------------------------------------------|
| Check the test results on the NQA client.                                  | <b>display nqa results</b> [ <i>admin-name test-name</i> ] |
| Check information about the task scheduling of the test on the NQA client. | <b>display nqa-schedule</b>                                |

NQA test results cannot be displayed automatically on the terminal. You can run the **display nqa results** command to check the results of the latest five tests.

Run the **display nqa results** command. If the following information is displayed, it means that the test succeeds.

- CtrlConnTime
- DataConnTime
- SumTime

```
<Quidway> display nqa results
1 . Test 1 result The test is finished
SendProbe :1 ResponseProbe:1
Completion :success RTD OverThresholds number: 0
MessageBodyOctetsSum :4498 Stats errors number: 0
Operation timeout number :0 System busy operation number:0
Drop operation number :0 Disconnect operation number: 0
CtrlConnTime Min/Max/Average:50/50/50
DataConnTime Min/Max/Average:40/40/40
SumTime Min/Max/Average :90/90/90
```

Run the **display nqa-schedule** command to check information about the task scheduling of the current NQA test instance.

```
<Quidway> display nqa-schedule
NQA Tests Max:2000 NQA Tests Num:1
 NQA Concurrent Requests Max:1000 NQA Concurrent Requests Num:0
 NQA Jitter Concurrent Max:5 NQA Jitter Concurrent Num:0
 NQA icmp Concurrent Max:50 NQA icmp Concurrent Num:0
 NQA Trace Concurrent Max:50 NQA Trace Concurrent Num:0
Index Schedule Time Type nqa icmp jitter packets
 1 start 2007-11-19 8:56:18 ftp 1 0 0 0
 2 end 2007-11-19 8:57:3 ftp 0 0 0 0
```

## 5.5 Configuring an FTP Upload Test

This section describes how to test the performance of the FTP upload function.

### Context

#### [5.5.1 Establishing the Configuration Tasks](#)

#### [5.5.2 Configuring the FTP Upload Test Parameters](#)

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

### 5.5.1 Establishing the Configuration Tasks

#### Applicable Environment

In the FTP upload test, the local device functions as an FTP client to upload the specified file to the FTP server.

Statistics about each FTP phase are displayed, including the time to set up FTP control connection and the time to transport the data.

In the FTP upload test, you can specify the file to be uploaded or the number of bytes to be uploaded. If certain number of bytes are specified, the FTP client can generate the test files automatically for uploading.

## Pre-configuration Tasks

Before configuring the FTP upload test, complete the following tasks:

- Configuring the FTP user name, password, and the login directory
- Configuring that the NQA client and the FTP server are reachable

## Data Preparation

To configure the FTP upload test, you need the following data.

| No. | Data                                                                                      |
|-----|-------------------------------------------------------------------------------------------|
| 1   | Administrator name and test name                                                          |
| 2   | IP address of the FTP server                                                              |
| 3   | Source IP address of the FTP operation                                                    |
| 4   | FTP user name and password                                                                |
| 5   | (Optional) VPN instance name and source and destination port numbers of the FTP operation |
| 6   | Name or size of the file to be uploaded                                                   |
| 7   | Start mode and end mode of the test                                                       |

## 5.5.2 Configuring the FTP Upload Test Parameters

### Context

Do as follows on the NQA client (FTP client).

### Procedure

- Step 1** Run the **system-view?** command to enter the system view.
- Step 2** Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.
- Step 3** Run the **test-type ftp** command to configure the test instance type as **FTP**.
- Step 4** Run the **destination-address ipv4** *ip-address* command to configure the destination IP address.
- Step 5** Run the **source-address ipv4** *ip-address* command to configure the source IP address.
- Step 6** (Optional) Run the following commands to configure other parameters for the FTP test.
- Run the **vpn-instance** *vpn-instance-name* command to configure a VPN test instance.
  - Run the **source-port** *port-number* command to configure the source port number.
  - Run the **destination-port** *port-number* command to configure the destination port number.

- Run the **sendpacket passroute** command to configure that the NQA test packets are sent without searching the routing table.

**Step 7** Run the **ftp-operation put** command to configure the FTP operation type as **put**.

**Step 8** Run the **ftp-username name** command to configure the FTP user name.

**Step 9** Run the **ftp-password password** command to configure the FTP password.

**Step 10** You can choose one of the following methods to upload the specified file.

- Run the **ftp-filename file-name** command to upload the specified file. If no file path is specified, the system searches the file in the current path. If the specified file name does not exist, a file is generated according to the specified file name, and the size of the file is specified as 1 MB.



#### NOTE

- The file path cannot contain such characters as ~, \*, /, \, ', ", and ,, but the file path can contain these characters.
- The file name can contain but cannot be only the extension name, such as .txt.
- If the file name does not contain an extension name, the system does not add one.
- Run the **ftp-filesize size** command to upload the file of specified size. The NQA client automatically generates a file named **nqa-ftp-test.txt** for uploading.



#### NOTE

During the FTP test, select a file of relatively small size. If the file is too large, the test may fail because of timeout.

**Step 11** Run the **start** command to start the NQA test.

The **start** command has several forms. You can choose one of the following forms as required:

- Run the **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]** command to start the test immediately.
- Run the **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]** command to start the test at a specified time.
- Run the **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]** command to start the test at a delayed time.

----End

## 5.5.3 Checking the Configuration

### Context

Run the following commands to check the previous configuration.

| Action                                    | Command                                                    |
|-------------------------------------------|------------------------------------------------------------|
| Check the test results on the NQA client. | <b>display nqa results</b> [ <i>admin-name test-name</i> ] |

| Action                                                                     | Command                     |
|----------------------------------------------------------------------------|-----------------------------|
| Check information about the task scheduling of the test on the NQA client. | <b>display nqa-schedule</b> |

NQA test results cannot be displayed automatically on the terminal. You can run the **display nqa results** command to check the results of the latest five tests.

Run the **display nqa results** command. If the following information is displayed, it means that the test succeeds.

- CtrlConnTime
- DataConnTime
- SumTime

```
<Quidway> display nqa results
NQA entry(admin, ftp) :testFlag is inactive ,testtype is ftp
1 . Test 1 result The test is finished
 SendProbe:1 ResponseProbe:1
 Completion :success RTD OverThresholds number: 0
 MessageBodyOctetsSum: 10240 Stats errors number: 0
 Operation timeout number: 0 System busy operation number:0
 Drop operation number:0 Disconnect operation number: 0
 CtrlConnTime Min/Max/Average: 70/70/70
 DataConnTime Min/Max/Average: 2580/2580/2580
 SumTime Min/Max/Average: 2650/2650/2650
```

Run the **display nqa-schedule** command to check information about the task scheduling of the current NQA test.

```
<Quidway> display nqa-schedule
NQA Tests Max:2000 NQA Tests Num:1
 NQA Concurrent Requests Max:1000 NQA Concurrent Requests Num:0
 NQA Jitter Concurrent Max:5 NQA Jitter Concurrent Num:0
 NQA icmp Concurrent Max:50 NQA icmp Concurrent Num:0
 NQA Trace Concurrent Max:50 NQA Trace Concurrent Num:0
 Index Schedule Time Type nqa icmp jitter packets
 1 start 2007-11-19 8:56:18 ftp 1 0 0 0
 2 end 2007-11-19 8:57:3 ftp 0 0 0 0
```

## 5.6 Configuring an HTTP Test

This section describes how to test the response speed of the HTTP service in each phase.

### Context

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

#### [5.6.2 Configuring the HTTP Test Parameters](#)

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

### 5.6.1 Establishing the Configuration Task

## Applicable Environment

Through the NQA HTTP test, you can obtain the responding speed in three phases:

- Time of Domain Name Server (DNS) resolution: It is a period from the time when the client sends the DNS packet to the resolver for resolving the name of the HTTP server to an IP address to the time when DNS resolution packets containing the IP address return.
- Time to set up a TCP connection: It is the time taken by the client to set up a TCP connection with the HTTP server through three-way handshake.
- Transaction time: It is a period from the time at which the client sends Get or Post packets to the HTTP server to the time at which the response packet sent by the client reaches the HTTP server.

## Pre-configuration Tasks

Before configuring the HTTP test, complete the following tasks:

- Configuring the HTTP server
- Configuring that the NQA client and the HTTP server are reachable.

## Data Preparation

To configure the HTTP test, you need the following data.

| No. | Data                                                                                            |
|-----|-------------------------------------------------------------------------------------------------|
| 1   | Administrator name and test name                                                                |
| 2   | Name of the HTTP server                                                                         |
| 3   | (Optional): Source port number, destination port number, and percentage of the failed NQA tests |
| 4   | HTTP operation type                                                                             |
| 5   | Webpage to be visited and the HTTP version                                                      |
| 6   | Start mode and end mode of the test                                                             |

## 5.6.2 Configuring the HTTP Test Parameters

### Context

Do as follows on the NQA client that also functions as an HTTP client:

### Procedure

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

**Step 2** Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.

**Step 3** Run the **test-type http** command to configure the test instance type as **http**.

**Step 4** Run the **destination-address ipv4 ip-address** command to configure the destination IP address.

**Step 5** (Optional) Run the following commands to configure other parameters for the HTTP test.

- Run the **vpn-instance vpn-instance-name** command to configure a VPN test instance.
- Run the **source-address ipv4 ip-address** command to configure the source IP address.
- Run the **source-port port-number** command to configure the source port number.
- Run the **destination-port port-number** command to configure the destination port number.

 **NOTE**

By default, the destination port number is 80.

- Run the **fail-percent percent** command to set the percentage of the failed NQA tests.
- Run the **sendpacket passroute** command to configure that the NQA test packets are sent without searching the routing table.

**Step 6** Run the **http-operation { get | post }** command to configure the HTTP operation type.

By default, the HTTP operation type is **get**.

**Step 7** Run the **http-url deststring [ verstring ]** command to configure the web page to be visited and the HTTP version.

 **NOTE**

- Run the **http-url deststring [ verstring ]**, and enter the web page name directly. If the entered information contains **http://** or domain name, the test instance fails.
- If no HTTP version is configured, HTTP1.0 is supported by default. You can configure to support HTTP1.1.

**Step 8** Run the **start** command to start the NQA test.

The **start** command has several forms. You can choose one of the following forms as required:

- Run the **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]** command to start the test immediately.
- Run the **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]** command to start the test at a specified time.
- Run the **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]** command to start the test at a delayed time.

----End

## 5.6.3 Checking the Configuration

### Context

Run the following commands to check the previous configuration.

| Action                                                                     | Command                                                    |
|----------------------------------------------------------------------------|------------------------------------------------------------|
| Check the test results on the NQA client.                                  | <b>display nqa results</b> [ <i>admin-name test-name</i> ] |
| Check information about the task scheduling of the test on the NQA client. | <b>display nqa-schedule</b>                                |

NQA test results cannot be displayed automatically on the terminal. You can run the **display nqa results** command to check the results of the latest five tests.

Run the **display nqa results** command. If the following information is displayed, it means that the test succeeds.

- "DNSRTT"
- "TCPConnectRTT"
- "TransactionRTT and RTT"

```
<Quidway> display nqa results
NQA entry(admin, http) :testFlag is inactive ,testtype is http
1 . Test 1 result The test is finished
 SendProbe:3 ResponseProb:3
 Completions: success OverThresholdsnumber: 0
 MessageBodyOctetsSum: 0 TargetAddress: 10.2.2.2
 DNSQueryError number: 0 HTTPError number: 0
 TcpConnError number : 3 System busy operation number:0
 DNSRTT Sum/Min/Max:0/0/0 TCPConnectRTT Sum/Min/Max: 7/2/3
 TransactionRTT Sum/Min/Max: 11/3/4 RTT Sum/Min/Max: 18/5/7
 DNSServerTimeout:0 TCPConnectTimeout:0 TransactionTimeout: 0
```

Run the **display nqa-schedule** command to check information about the task scheduling of the current NQA test.

```
<Quidway> display nqa-schedule
NQA Tests Max:2000
NQA Concurrent Requests Max:1000
NQA Jitter Concurrent Max:5
NQA icmp Concurrent Max:50
NQA Trace Concurrent Max:50
Index Schedule Time Type nqa icmp jitter packets
1 start 2007-11-19 8:56:18 http 1 0 0 0
2 end 2007-11-19 8:57:3 http 0 0 0 0
NQA Tests Num:1
NQA Concurrent Requests Num:0
NQA Jitter Concurrent Num:0
NQA icmp Concurrent Num:0
NQA Trace Concurrent Num:0
```

## 5.7 Configuring the SNMP Query Test

This section describes how to test the status of the communication between hosts and SNMP agents.

### Context

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

#### [5.7.2 Setting Parameters for the SNMP Query Test](#)

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

## 5.7.1 Establishing the Configuration Task

### Context

### Applicable Environment

Through the SNMP Query test, you can obtain the statistics of the communication between hosts and SNMP agents.

### Pre-configuration Tasks

Before configuring the SNMP Query test, complete the following tasks:

- Configuring the SNMP agent
- Configuring routes between the NQA client and the SNMP agent

### Data Preparation

To configure the SNMP query test, you need the following data.

| No. | Data                                                                                                                                              |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Administrator name and test name                                                                                                                  |
| 2   | IP address of the SNMP agent                                                                                                                      |
| 3   | (Optional) Source IP addresses and source port numbers of test packets, interval for sending test packets, and percentage of the failed NQA tests |
| 4   | Start mode and end mode of the test                                                                                                               |

## 5.7.2 Setting Parameters for the SNMP Query Test

### Context

Do as follows on the NQA client.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.
- Step 3** Run the **test-type snmp** command to set the type of the test instance to **snmp**.
- Step 4** Run the **destination-address ipv4** *ip-address* command to set the destination IP address, that is, IP address of the SNMP agent.

**NOTE**

The SNMP function must be enabled on the destination host, otherwise, the destination host fails to receive response packets.

**Step 5** (Optional) Perform the following tasks to set other parameters for SNMP test instances:

- Run the **vpn-instance** *vpn-instance-name* command to set the name of the VPN instance.
- Run the **source-address ipv4** *ip-address* command to set the source IP address.
- Run the **source-port** *port-number* command to set the source port number.
- Run the **interval seconds** *interval* command to set an interval for sending test packets.
- Run the **fail-percent** *percent* command to set the percentage of the failed NQA test.
- Run the **sendpacket passroute** command to configure an NQA test instance to send packets without searching the routing table.

**Step 6** Run the **start** command to start an NQA test instance.

The **start** command has several forms. You can choose one of the following forms as required:

- Run the **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start a test instance immediately.
- Run the **start at** [ *yyyy/mm/dd* ] *hh:mm:ss* [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start a test instance at a specified time.
- Run the **start delay** { **seconds** *second* | *hh:mm:ss* } [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start a test instance at a delayed time.

----End

## 5.7.3 Checking the Configuration

### Context

Run the following commands to check the previous configuration.

| Action                                                                     | Command                                                |
|----------------------------------------------------------------------------|--------------------------------------------------------|
| View the test results on the NQA client.                                   | <b>display nqa results</b> <i>admin-name test-name</i> |
| View information about the scheduling of the test tasks on the NQA client. | <b>display nqa-schedule</b>                            |

**NOTE**

NQA test results cannot be displayed automatically on a terminal. You must run the **display nqa results** command to view test results. The command output contains the records of the latest five tests.

Run the **display nqa results** command. If the following is displayed, it means that the test succeeds.

```
<Quidway> display nqa results
NQA entry(admin, snmp) :testFlag is inactive ,testtype is snmp
```

```
1 . Test 1 result The test is finished
Send operation times: 3 Receive response times: 3
Completion:succcess RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:172.16.255.5
Min/Max/Average Completion Time: 10/30/16
Sum/Square-Sum Completion Time: 50/1100
Last Good Probe Time: 2008-8-2 4:13:19.4
```

## 5.8 Configuring a TCP Test

This section describes how to test the response speed of the TCP interface.

### Context

[5.8.1 Establishing the Configuration Task](#)

[5.8.2 Configuring the TCP Server](#)

[5.8.3 Configuring the TCP Client](#)

[5.8.4 Checking the Configuration](#)

### 5.8.1 Establishing the Configuration Task

#### Applicable Environment

To test the time for a specified interface to respond to a TCP connection request, you can create a TCP test instance.

#### Pre-configuration Tasks

Before configuring the TCP test, configure that the NQA client and the TCP server are reachable.

#### Data Preparation

To configure the TCP test, you need the following data.

| No. | Data                                                                                                                                                    |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Administrator name and test name                                                                                                                        |
| 2   | IP address and port number monitored by the TCP server                                                                                                  |
| 3   | Destination IP addresses of the probe packets sent by the TCP client                                                                                    |
| 4   | (Optional) Destination port number, source IP addresses, source port numbers, interval for sending test packets, and percentage of the failed NQA tests |
| 5   | Start mode and end mode of the test                                                                                                                     |

## 5.8.2 Configuring the TCP Server

### Context

Do as follows on the NQA client:

### Procedure

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

**Step 2** Run the **nqa-server tcpconnect** [ **vpn-instance** *vpn-instance-name* ] *ip-address port-number* command to configure the TCP monitoring service.

The IP address and interface number monitored by the server must be consistent with those configured on the client.

----End

## 5.8.3 Configuring the TCP Client

### Context

Do as follows on the NQA client.

### Procedure

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

**Step 2** Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.

**Step 3** Run the **test-type tcp** command to configure the test instance type as **tcp**.

**Step 4** Run the **destination-address ipv4** *ip-address* command to configure the destination IP address.

**Step 5** Run the **destination-port** *port-number* command to configure the destination port number.

**Step 6** (Optional) Run the following commands to configure other parameters for the TCP test.

- Run the **vpn-instance** *vpn-instance-name* command to configure a VPN test instance.
- Run the **source-address ipv4** *ip-address* command to configure the source IP address.
- Run the **source-port** *port-number* command to configure the source interface number.
- Run the **interval seconds** *interval* command to configure intervals for sending test packets.
- Run the **fail-percent** *percent* command to set the percentage of the failed NQA tests.
- Run the **sendpacket passroute** command to configure that the NQA test packets are sent without searching the routing table.

**Step 7** Run the **start** command to start the NQA test.

The **start** command has several forms. You can choose one of the following forms as required:

- Run the **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start the test immediately.

- Run the **start at** [ yyyy/mm/dd ] hh:mm:ss [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ] command to start the test at a specified time.
- Run the **start delay** { **seconds** second | hh:mm:ss } [ **end** { **at** [ yyyy/mm/dd ] hh:mm:ss | **delay** { **seconds** second | hh:mm:ss } | **lifetime** { **seconds** second | hh:mm:ss } } ] command to start the test at a delayed time.

The differences between the TCP public tests and the TCP private tests are as follows:

- The TCP public tests do not require that the destination port be configured on the client. Connection requests are initiated and sent to the TCP port 7 of the destination address. The server should monitor the TCP port 7.
- TCP private test requires that the destination port be specified and the monitoring be enabled on the server.

----End

## 5.8.4 Checking the Configuration

### Context

Run the following commands to check the previous configuration.

| Action                                                                     | Command                                                    |
|----------------------------------------------------------------------------|------------------------------------------------------------|
| Check the test results on the NQA client.                                  | <b>display nqa results</b> [ <i>admin-name test-name</i> ] |
| Check information about the server on the NQA server.                      | <b>display nqa-server</b>                                  |
| Check information about the task scheduling of the test on the NQA client. | <b>display nqa-schedule</b>                                |

NQA test results cannot be displayed automatically on the terminal. You can run the **display nqa results** command to check the results of the latest five tests.

Run the **display nqa results** command. If the following information is displayed, it means that the test succeeds.

```
<Quidway> display nqa results
NQA entry(admin, tcp) :testFlag is inactive ,testtype is tcp
1 . Test 1 result The test is finished
 Send operation times: 3 Receive response times: 3
 Completion:success RTD OverThresholds number: 0
 Attempts number:1 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:0
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:3.1.1.1
 Min/Max/Average Completion Time: 10/20/13
 Sum/Square-Sum Completion Time: 40/600
 Last Good Probe Time: 2008-1-2 2:31:11.9
```

Run the **display nqa-server** command to check the status of the server.

```
<Quidway> display nqa-server
NQA Server Max:5000 NQA Server Num:1
NQA Concurrent TCP Server:1 NQA Concurrent UDP Server:0
nqa-server tcpconnect 3.1.1.1 180 Active
```

Run the **display nqa-schedule** command to check information about the task scheduling of the current NQA test.

```
<Quidway> display nqa-schedule
NQA Tests Max:2000 NQA Tests Num:1
NQA Concurrent Requests Max:1000 NQA Concurrent Requests Num:0
NQA Jitter Concurrent Max:5 NQA Jitter Concurrent Num:0
NQA icmp Concurrent Max:50 NQA icmp Concurrent Num:0
NQA Trace Concurrent Max:50 NQA Trace Concurrent Num:0
Index Schedule Time Type nqa icmp jitter packets
1 start 2007-11-19 8:56:18 tcp 1 0 0 0
2 end 2007-11-19 8:57:3 tcp 0 0 0 0
```

## 5.9 Configuring a UDP Test

This section describes how to test the response speed of the UDP port.

### Context

[5.9.1 Establishing the Configuration Task](#)

[5.9.2 Configuring the UDP Server](#)

[5.9.3 Configuring the UDP Client](#)

[5.9.4 Checking the Configuration](#)

### 5.9.1 Establishing the Configuration Task

#### Applicable Environment

To obtain the time for the specified interface to respond to a UDP connection request, you can create a UDP test instance.

#### Pre-configuration Tasks

Before configuring the UDP test, configure the NQA client and the UDP server to be reachable.

#### Data Preparation

To configure the UDP test, you need the following data.

| No. | Data                                                                 |
|-----|----------------------------------------------------------------------|
| 1   | Administrator name and name of the test instance                     |
| 2   | IP address and number of the port monitored by the UDP server        |
| 3   | Destination IP addresses of the probe packets sent by the UDP client |

| No. | Data                                                                                                                                                     |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4   | (Optional) Destination port numbers, source IP addresses, source port numbers, interval for sending test packets, and percentage of the failed NQA tests |
| 5   | Start mode and end mode of the test                                                                                                                      |

## 5.9.2 Configuring the UDP Server

### Context

Do as follows on the NQA server.

### Procedure

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

**Step 2** Run the **nqa-server udpecho** [ *vpn-instance-name* ] *ip-address port-number* command to configure the UDP monitoring service.

The IP address and number of the port monitored by the server must be consistent with those configured on the client.

----End

## 5.9.3 Configuring the UDP Client

### Context

Do as follows on the NQA client:

### Procedure

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

**Step 2** Run the **nqa test-instance** *admin-name test-name* command to create an NQA test and enter the test instance view.

**Step 3** Run the **test-type ftp** command to configure the test type as **udp**.

**Step 4** Run the **destination-address ipv4** *ip-address* command to configure the destination IP address.

**Step 5** Run the **destination-port** *port-number* command to configure the destination port number.

**Step 6** (Optional) Run the following commands to configure other parameters for the UDP test.

- Run the **vpn-instance** *vpn-instance-name* command to configure a VPN test instance.
- Run the **source-address ipv4** *ip-address* command to configure the source IP address.
- Run the **source-port** *port-number* command to configure the source port number.
- Run the **interval seconds** *interval* command to configure the interval for sending test packets.

- Run the **fail-percent** *percent* command to set the percentage of the failed NQA tests.
- Run the **sendpacket passroute** command to configure the NQA test packets to be sent directly without searching the routing table.

**Step 7** Run the **start** command to start the NQA test.

The **start** command has several forms. You can choose one of the following forms as required:

- Run the **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start the test immediately.
- Run the **start at** [ *yyyy/mm/dd* ] *hh:mm:ss* [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start the test at a specified time.
- Run the **start delay** { **seconds** *second* | *hh:mm:ss* } [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start the test at a delayed time.

The differences between the UDP Public tests and the UDP Private tests are as follows:

- The UDP Public tests do not require that the destination port be configured on the client. Connection requests are initiated and sent to UDP port 7 of the destination address. The server should monitor UDP port 7.
- The UDP Private test requires that the destination port be specified and the monitoring be enabled on the server.

----End

## 5.9.4 Checking the Configuration

### Context

Run the following commands to check the previous configuration.

| Action                                                                     | Command                                                    |
|----------------------------------------------------------------------------|------------------------------------------------------------|
| Check the test results on the NQA client.                                  | <b>display nqa results</b> [ <i>admin-name test-name</i> ] |
| Check information about the server on the NQA server.                      | <b>display nqa-server</b>                                  |
| Check information about the task scheduling of the test on the NQA client. | <b>display nqa-schedule</b>                                |

NQA test results cannot be displayed automatically on the terminal. You can run the **display nqa results** command to check the results of the latest five tests.

Run the **display nqa results** command. If the following information is displayed, it means that the test succeeds.

```
<Quidway> display nqa results
NQA entry(admin, udp) :testFlag is active ,testtype is udp
1 . Test 1 result The test is finished
```

```

Send operation times: 3 Receive response times: 3
Completion:success RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:3.1.1.1
Min/Max/Average Completion Time: 1/10/4
Sum/Square-Sum Completion Time: 12/102
Last Good Probe Time: 2008-1-2 3:26:5.9

```

Run the **display nqa-server** command to check the status of the server.

```

<Quidway> display nqa-server
NQA Server Max:5000 NQA Server Num:1
NQA Concurrent TCP Server:0 NQA Concurrent UDP Server:1
nqa-server udpecho 3.1.1.1 2000 Active

```

Run the **display nqa-schedule** command to check information about the task scheduling of the current NQA test.

```

<Quidway> display nqa-schedule
NQA Tests Max:2000 NQA Tests Num:1
NQA Concurrent Requests Max:1000 NQA Concurrent Requests Num:0
NQA Jitter Concurrent Max:5 NQA Jitter Concurrent Num:0
NQA icmp Concurrent Max:50 NQA icmp Concurrent Num:0
NQA Trace Concurrent Max:50 NQA Trace Concurrent Num:0
Index Schedule Time Type nqa icmp jitter packets
1 start 2007-11-19 8:56:18 udp 1 0 0 0
2 end 2007-11-19 8:57:3 udp 0 0 0 0

```

## 5.10 Configuring a Jitter Test

This section describes how to test the jitter of processing UDP packets.

### Context

[5.10.1 Establishing the Configuration Task](#)

[5.10.2 Configuring the Jitter Server](#)

[5.10.3 Configuring the Jitter Client](#)

[5.10.4 Checking the Configuration](#)

### 5.10.1 Establishing the Configuration Task

#### Applicable Environment

Jitter time refers to the interval for receiving two adjacent packets minus the interval for sending the two packets.

The process of the Jitter test is as follows:

- The source sends packets to the destination end after a specific interval.
- After receiving a packet, the destination end adds a timestamp to the packet and returns it to the source end.

- After receiving the returned packets, the source end obtains the jitter time by subtracting the interval for sending the packets from the interval for the destination to receive the packets.

The maximum, minimum, and average jitter time are calculated according to the information received on the source. As a result, the maximum unidirectional delay is obtained, and thus the network status is clearly shown.

In the jitter test, you can set the number of packets to be sent consecutively in each test. Through this setting, certain traffic can be simulated. For example, send 3000 UDP packets at intervals of 20 milliseconds. Then, in 1 minute, G.711 traffic is simulated.

#### NOTE

Configuring NTP on the client and the server can effectively improve the accuracy of the test.

## Pre-configuration Tasks

Before configuring the jitter test, configure the NQA client and the UDP server to be reachable.

## Data Preparation

To configure the Jitter test, you need the following data.

| No. | Data                                                                                                                                                                                                                                                                                         |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Administrator name and test name                                                                                                                                                                                                                                                             |
| 2   | IP address and number of the port monitored by the UDP server                                                                                                                                                                                                                                |
| 3   | Destination IP address and port number of the probe packets sent by the UDP client                                                                                                                                                                                                           |
| 4   | (Optional) Name of a VPN instance, source IP address and source port that sends test packets, number of the test probes sent each time, number of the test packets sent each time, interval for sending test packets, and percentage of the failed NQA tests, version of the jitter packets. |
| 5   | Start mode and end mode of the test                                                                                                                                                                                                                                                          |

## 5.10.2 Configuring the Jitter Server

### Context

Do as follows on the NQA server.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **nqa-server udpecho ip-address port-number** command to configure the UDP monitoring service.

The IP address and number of the port monitored by the server must be consistent with those configured on the client.

----End

## 5.10.3 Configuring the Jitter Client

### Context



#### NOTE

The system supports maximum unidirectional delay of the Jitter test.

Do as follows on the NQA client:

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **nqa test-instance** *admin-name test-name* command to create an NQA test and enter the test instance view.
- Step 3** Run the **test-type jitter** command to configure a Jitter test.
- Step 4** Run the **destination-address ipv4** *ip-address* command to configure the destination IP address.
- Step 5** Run the **destination-port** *port-number* command to configure the destination interface number.
- Step 6** (Optional) Run the following commands to configure other parameters for the Jitter test.
  - Run the **vpn-instance** *vpn-instance-name* command to configure a VPN test instance.
  - Run the **source-address ipv4** *ip-address* command to configure the source IP address.
  - Run the **source-port** *port-number* command to configure the source interface number.
  - Run the **probe-count** *number* command to set the number of test probes sent each time.
  - Run the **jitter-packetnum** *number* command to set the number of test packets sent during each test.

The Jitter test is used to collect statistics of and analyze the transmission delay variation of the UDP packets. The system sends multiple test packets for each test to make the statistics more accurate. The more test packets are sent, the more accurate the statistics are. The period that lasts, however, is longer.



#### NOTE

The **probe-count** command is used to configure the number of the Jitter tests whereas the **jitter-packetnum** command configures the number of the test packets sent during each test. During the actual configuration, the product of the number of the Jitter tests multiplied by the number of the test packets must be less than 3000.

- Run the **interval** { **milliseconds** *interval* | **seconds** *interval* } command to set the interval for sending test packets.

The shorter the interval for sending test packets, the faster the test is completed. Sending and receiving test packets may be delayed. Therefore, if the interval for sending test packets is set to a small value, a relatively great error may occur in the statistics of the Jitter test.
- Run the **fail-percent** *percent* command to set the percentage of the failed NQA tests.

- Run the **sendpacket passroute** command to configure the NQA test packets to be sent without searching the routing table.
- Run the **nqa-jitter tag-version { 1 | 2 }** command to configure the version of the Jitter test packets in the system view.

After collecting the packet loss across a uni-directional link is enabled, you can find the packet loss across the link from the source to the destination (or from the destination to the source or from an unknown direction). According to these statistics, the network administrator can easily locate network faults and detect malicious attacks.

**Step 7** Run the **start** command to start the NQA test.

The **start** command has several forms. You can choose one of the following forms as required:

- Run the **start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]** command to start the test immediately.
- Run the **start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]** command to start the test at a specified time.
- Run the **start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]** command to start the test at a delayed time.

----End

## 5.10.4 Checking the Configuration

### Context

Run the following commands to check the previous configuration.

| Operations                                                                 | Commands                                                   |
|----------------------------------------------------------------------------|------------------------------------------------------------|
| Check the test results on the NQA client.                                  | <b>display nqa results</b> [ <i>admin-name test-name</i> ] |
| Check information about the server on the NQA server.                      | <b>display nqa-server</b>                                  |
| Check information about the task scheduling of the test on the NQA client. | <b>display nqa-schedule</b>                                |

NQA test results cannot be displayed automatically on the terminal. You can run the **display nqa results** command to check the results of the latest five tests.

Run the **display nqa results** command. If the following information is displayed, it means that the test succeeds.

```
<Quidway> display nqa results admin jitter
NQA entry(admin, jitter) :testFlag is inactive ,testtype is jitter
 1 . Test 1 result The test is finished
 SendProbe:60 ResponseProbe:60
 Completion :success RTD OverThresholds number:0
```

```

Min/Max/Sum RTT:1/30/257
NumOfRTT:60
Operation sequence errors number:0
System busy operation number:0
Min Positive SD:10
Max Positive SD:30
Positive SD Number:8
Positive SD Sum:100
Positive SD Square Sum :1600
Min Negative SD:10
Max Negative SD:30
Negative SD Number:7
Negative SD Sum:110
Negative SD Square Sum :2100
Packet Loss SD:0
Max Delay SD:15
jitter out value:2.7790723
OWD OverThresholds number:0
NumberOfOWD:60
OWD SD Sum:105

RTT Square Sum:4347
Drop operation number:0
RTT Stats errors number:0
Operation timeout number:0
Min Positive DS:10
Max Positive DS:20
Positive DS Number:5
Positive DS Sum:60
Positive DS Square Sum :800
Min Negative DS:10
Max Negative DS:20
Negative DS Number:5
Negative DS Sum:60
Negative DS Square Sum :800
Packet Loss DS:0
Max Delay DS:14
jitter in value:1.6327616
Packet Loss Unknown:0
OWD DS Sum:92

```



#### NOTE

When the delay of the test packets sent from the source end is longer than that from the destination end, the Jitter value is negative.

Run the **display nqa-schedule** command to check information about the task scheduling of the current NQA test.

```

<Quidway> display nqa-schedule
NQA Tests Max:2000
NQA Concurrent Requests Max:1000
NQA Jitter Concurrent Max:5
NQA icmp Concurrent Max:50
NQA Trace Concurrent Max:50
Index Schedule Time
1 start 2007-11-19 8:56:18
2 end 2007-11-19 8:57:3

NQA Tests Num:1
NQA Concurrent Requests Num:0
NQA Jitter Concurrent Num:0
NQA icmp Concurrent Num:0
NQA Trace Concurrent Num:0
Type nqa icmp jitter packets
jitter 1 0 0 0
jitter 0 0 0 0

```

## 5.11 Configuring an NQA Test Group

This section describes how to configure an NQA test group.

### Context

[5.11.1 Establishing the Configuration Task](#)

[5.11.2 Configuring an NQA Test Group](#)

[5.11.3 Checking the Configuration](#)

### 5.11.1 Establishing the Configuration Task

#### Applicable Environment

To perform ICMP or jitter tests for several destinations, configure NQA test groups. That is, group the tests of the same type for uniform administration.

#### Pre-configuration Tasks

Before configuring the NQA test group, configure the NQA client and the tested device to be reachable.

## Data Preparation

To configure the NQA test group, you need the following data.

| No. | Data                                                   |
|-----|--------------------------------------------------------|
| 1   | Administrator name and test name                       |
| 2   | Administrator names and test names of the test members |
| 3   | Optional ICMP and jitter test parameters               |
| 4   | (Optional) Test period of the test group               |
| 5   | Start mode and end mode of the test                    |

### NOTE

- When a test instance initiates a test group, it becomes the leader automatically. Other test instances join the group to perform tests as test members.
- In the test group, the group leader does not perform tests. The leader administrates only the frequency of tests, timeout period, interval for sending test packets, group test period. The test members configure only the source IP address, source port number, destination IP address, and destination port number.
- If the size of the packet is not set to the default value before the test member joins the test group, it remains unchanged afterwards. If the size is set to the default value, the configuration of the test group is adopted.
- If a VPN test instance is configured before the test member joins the test group, the VPN test instance remains unchanged afterwards. If no VPN test instance is configured, the VPN test instance configured by the test group is adopted.
- For those configurations that the test instance does not support, the test member adopts the configuration of the test group.
- After the test member leaves a test group, the source IP address, source port number, destination IP address, and destination port number remain whereas other parameters are restored to the default values.

## 5.11.2 Configuring an NQA Test Group

### Context

Do as follows on the NQA client.

### NOTE

For other necessary configurations required by the test group type, see [5.2 Configuring an ICMP Test](#) and [5.10 Configuring a Jitter Test](#).

### Procedure

- Step 1** Run the **system-view?** command to enter the system view.
- Step 2** Run the **nqa test-instance** *admin-name test-name* command to create an NQA test and enter the test instance view.
- Step 3** Run the **test-type { icmp | jitter }** command to configure the test type.

By default, the NQA test type is ICMP.

**Step 4** Run the **switch-to group** command to upgrade the current test instance to a test group.

**Step 5** Run the **quit** command to return to the system view.

**Step 6** Run the **nqa test-instance** *admin-name test-name* command to enter the NQA test instance view.

**Step 7** Run the **join group nqa** *admin-name test-name* command to add the current NQA test instance to the newly-created test group.

 **NOTE**

For other necessary configurations required by the test instance type, see [5.2 Configuring an ICMP Test](#) and [5.10 Configuring a Jitter Test](#).

**Step 8** Run the **quit** command to return to the system view.

**Step 9** Run the **nqa test-instance** *admin-name test-name* command to enter the NQA test group view.

 **NOTE**

For other necessary configurations required by the test group type, see [5.2 Configuring an ICMP Test](#) and [5.10 Configuring a Jitter Test](#).

**Step 10** (Optional) Run the **group-testperiod** *period* command to configure the test period of the test group.

By default, the test period of the NQA test group is 60s.

 **NOTE**

During the specified period for the group test, if there are too many members in the test group, the group test cannot be started normally. Therefore, you should select a proper period for the group test according to the number of the group members.

**Step 11** Run the **start** command to start the NQA test.

The **start** command has several forms. You can choose one of the following forms as required:

- Run the **start now** [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start the test immediately.
- Run the **start at** [ *yyyy/mm/dd* ] *hh:mm:ss* [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start the test at a specified time.
- Run the **start delay** { **seconds** *second* | *hh:mm:ss* } [ **end** { **at** [ *yyyy/mm/dd* ] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } } ] command to start the test at a delayed time.

**end delay:** Information about whether a test succeeds or fails is displayed after some delay. If the default value is specified as 0, there is no delay. **lifetime:** The duration for a test is configured. By default, the duration is not configured. When the duration ends, the test is forcibly stopped, and **no result** is displayed.

----End

## 5.11.3 Checking the Configuration

### Context

Run the following commands to check the previous configuration.

| Operations                               | Commands                                                   |
|------------------------------------------|------------------------------------------------------------|
| View the test results on the NQA client. | <b>display nqa results</b> [ <i>admin-name test-name</i> ] |
| View the test status on the NQA client.  | <b>display nqa-agent</b>                                   |

You can run the **display nqa results** command to check the test result of the NQA test members instead of the test group.

After the test group is created, run the **display nqa-agent** command. You can view to which test group the test member belongs to according to the "nqa status" field in the command output.

## 5.12 Configuring Universal NQA Test Parameters

This section describes how to configure universal parameters for NQA tests.

### Context

[5.12.1 Establishing the Configuration Task](#)

[5.12.2 Configuring the Universal NQA Test Parameters](#)

[5.12.3 Checking the Configuration](#)

### 5.12.1 Establishing the Configuration Task

#### Applicable Environment

NQA supports not only the setting of the parameters for various test types, but also the setting of universal parameters of tests.

In general use, the default setting of the universal parameters are adopted.

#### Pre-configuration Tasks

Before configuring universal NQA parameters, create NQA tests correctly.

#### Data Preparation

To configure the universal NQA parameters, you need the following data.

| No. | Data                                          |
|-----|-----------------------------------------------|
| 1   | Description of tests                          |
| 2   | Timeout period of tests                       |
| 3   | Number of probe packets sent during each test |
| 4   | NQA test period                               |

| No. | Data                                      |
|-----|-------------------------------------------|
| 5   | Whether the test packet can be fragmented |
| 6   | Maximum history records to be reserved    |
| 7   | Maximum history records to be reserved    |
| 8   | Aging time of tests                       |

## 5.12.2 Configuring the Universal NQA Test Parameters

### Context

Do as follows on the NQA client.

### Procedure

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

**Step 2** Run the **nqa test-instance** *admin-name test-name* command to enter the view of an NQA test instance.

**Step 3** Perform the following as required to configure universal parameters:

- Run the **description** *string* command to set the description of the test instance.
- Run the **timeout** *time* command to set the timeout period of the test.
- Run the **probe-count** *number* command to set the number of test probes sent during each test.



**NOTE**

This parameter is invalid for the FTP test.

- Run the **frequency** *interval* command to set the test period.
- Run the **set-df** command to forbid fragmentation of packets.



**NOTE**

The **set-df** command can be used only for the Traceroute test.

- Run the **records history** *number* command to configure the maximum history records to be reserved.
- Run the **records result** *number* command to configure the maximum test results to be reserved.
- Run the **agetime** *hh:mm:ss* command to configure the aging time of the test.

----End

## 5.12.3 Checking the Configuration

### Context

Run the following command to check the previous configuration.

| Action                                            | Command                                                                                              |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Check the universal parameters set for NQA tests. | <b>display nqa-agent</b> [ <b>test-instance</b> <i>admin-name operation-tag</i> ] [ <b>verbose</b> ] |

## 5.13 Configuring the Bidirectional Transmission Delay Threshold

This section describes how to configure the bidirectional transmission delay threshold for an NQA test.

### Context

[5.13.1 Establishing the Configuration Task](#)

[5.13.2 Configuring the Bidirectional Transmission Delay Threshold](#)

[5.13.3 Checking the Configuration](#)

### 5.13.1 Establishing the Configuration Task

#### Applicable Environment

If the bidirectional transmission delay threshold is configured for an NQA test instance, the statistics on the test packets that exceed the set threshold are shown. This provides a basis for the network manager to analyze the operation status of the specified service.

#### Pre-configuration Tasks

Before configuring the NQA threshold, complete the following tasks:

- Checking that the device runs normally
- Creating the NQA test instance and setting related parameters

#### Data Preparation

To configure the bidirectional transmission delay threshold, you need the following data.

| No. | Data                                       |
|-----|--------------------------------------------|
| 1   | Administrator name and test name           |
| 2   | Bidirectional transmission delay threshold |

### 5.13.2 Configuring the Bidirectional Transmission Delay Threshold

## Context

Do as follows on the S-switch to perform NQA tests.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **nqa test-instance** *admin-name test-name* command to enter the NQA test instance view.
- Step 3** Run the **threshold rtd** *value* command to configure the bidirectional transmission delay threshold.
- Step 4** Run the **send-trap overthreshold** command to enable the trap function.

----End

## 5.13.3 Checking the Configuration

### Context

Run the following command to check the previous configuration.

| Action                                                                           | Command                    |
|----------------------------------------------------------------------------------|----------------------------|
| Check the bidirectional transmission delay threshold configured for an NQA test. | <b>display nqa results</b> |

Run the **display nqa-agent test-instance** *admin-name test-name verbose* command. If information about the bidirectional transmission delay threshold is displayed, it means that the configuration succeeds. For example:

```
<Quidway> display nqa-agent test-instance test jitter verbose
1 NQA entry(admin, jitter):
 test type:icmp current flag:inactive
 current status:no start current completion:no result
 start at : no start time end at : no end time
 nqa status : normal
 configuration :
 test-type icmp
 destination-address ipv4 3.1.1.1
 threshold rtd 2
 sendpacket passroute
```

## 5.14 Configuring the Unidirectional Transmission Delay Threshold

This section describes how to configure the unidirectional transmission delay threshold for an NQA test.

## Context

[5.14.1 Establishing the Configuration Task](#)

[5.14.2 Configuring the Unidirectional Transmission Delay Threshold](#)

[5.14.3 Checking the Configuration](#)

## 5.14.1 Establishing the Configuration Task

### Applicable Environment

In jitter tests, after the unidirectional transmission delay threshold is configured, the statistics on the test packets that exceed the set threshold are shown. This provides a basis for the network manager to analyze the operation status of the specified service.

### Pre-configuration Tasks

Before configuring the unidirectional transmission delay threshold, complete the following tasks:

- Checking that the device is running normally
- Creating the NQA test and setting related parameters

### Data Preparation

To configure the unidirectional transmission delay threshold, you need the following data.

| No. | Data                             |
|-----|----------------------------------|
| 1   | Administrator name and test name |
| 2   | Threshold for a test             |

## 5.14.2 Configuring the Unidirectional Transmission Delay Threshold

### Context

Do as follows on the S-switch to perform NQA tests.

### Procedure

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

**Step 2** Run the **nqa test-instance** *admin-name test-name* command to enter the NQA view.

**Step 3** Run the **threshold owd** *owd-vale* command to configure the unidirectional transmission delay threshold.

----End

## 5.14.3 Checking the Configuration

### Context

Run the following command to check the previous configuration.

| Action                                                                            | Command                                                                           |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Check the unidirectional transmission delay threshold configured for an NQA test. | <b>display nqa-agent test-instance</b> <i>admin-name test-name</i> <b>verbose</b> |

Run the **display nqa-agent test-instance** *admin-name test-name* **verbose** command. If information about the uni-directional transmission delay threshold is displayed, it means that the configuration succeeds. For example:

```
<Quidway> display nqa-agent test-instance test jitter verbose
1 NQA entry(test, jitter):
 test type:jitter current flag:inactive
 current status:finished current completion:success
 start at : no start time end at : no end time
 nqa status : normal
 configuration :
 test-type jitter
 destination-address ipv4 10.1.1.2
 destination-port 2900
 threshold owd 20
 send-trap overthreshold
```

## 5.15 Configuring the Trap Function

This section describes how to configure the trap function in an NQA test.

### Context

[5.15.1 Establishing the Configuration Task](#)

[5.15.2 Enabling the Trap Function for Test Failures](#)

[5.15.3 Enabling the Trap Function for Probe Failures](#)

[5.15.4 Enabling the Trap Function for Probe Successes](#)

[5.15.5 Enabling the Trap Function When the Transmission Delay Exceeds the Threshold](#)

[5.15.6 Checking the Configuration](#)

### 5.15.1 Establishing the Configuration Task

## Applicable Environment

Traps are generated no matter whether the NQA test succeeds or fails. You can determine whether traps are sent to the NMS by enabling or disabling the trap function.

NQA supports three types of traps as defined in DISMAN-PING-MIB.

- Statistics on errors
  - Number of unroutable connections
  - Times of incorrect sequences
  - Timeout times of the test packets
- History statistics of each test packet
  - Timestamp added when each test packet is sent
  - Timestamp added when each test packet is received
  - Packets status displayed on the NQA client
- Statistics of results of each test
  - Number of times of successful tests
  - Sum of the response time of tests
  - Round Trip Time (RTT) square sum
  - Minimum RTT and maximum RTT of the packet
  - Destination IP address.
  - Number of the received response packets and the sent packets
  - Time when the last packet is received
- 

NQA also supports the sending of traps to the NMS when the uni-directional transmission delay or the bi-directional transmission delay exceeds the threshold.

- For all tests, if the bi-directional transmission delay exceeds the threshold and the trap function is enabled, traps are sent to the NMS with the specified IP address.
- For all the Jitter tests, if the uni-directional transmission delay exceeds the threshold and the trap function is enabled, traps are sent to the NMS with the specified IP address.

Traps carry such information: destination IP addresses, operation status, destination IP address of the test packet, minimum RTT, maximum RTT and total RTT, number of sent probe packets, number of received packets, RTT square sum, and time of the latest successful probe.

## Pre-configuration Tasks

Before configuring the Trap function, complete the following tasks:

- Configuring that the NQA client and the NMS are reachable
- Creating the NQA test and configuring related parameters

## Data Preparation

To configure the trap function, you need the following data.

| No. | Data                                                                                                                                                                                   |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Administrator name and test name                                                                                                                                                       |
| 2   | NQA events that trigger sending traps                                                                                                                                                  |
| 3   | <ul style="list-style-type: none"><li>• (Optional) Number of failed tests that trigger sending traps</li><li>• (Optional) Number of failed probes that trigger sending traps</li></ul> |

## 5.15.2 Enabling the Trap Function for Test Failures

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.
- Step 3** Run the **send-trap testfailure** command to enable the trap function.
- By default, the device is disabled from sending traps.
- Step 4** Run the **test-failtimes** *times* command to configure the number of test failures that triggers sending traps.
- By default, a trap is sent for each test failure.
- End

## 5.15.3 Enabling the Trap Function for Probe Failures

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **nqa test-instance** *admin-name test-name* command to create an NQA test and enter the test instance view.
- Step 3** Run the **send-trap probefailure** command to enable the trap function.
- By default, the device is disabled from sending traps.
- Step 4** Run the **probe-failtimes** *times* command to configure the number of probe failures that triggers sending traps.
- By default, a trap is sent for each probe failure.
- End

## 5.15.4 Enabling the Trap Function for Probe Successes

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **nqa test-instance** *admin-name test-name* command to create an NQA test and enter the test instance view.
- Step 3** Run the **send-trap testcomplete** command to enable the trap function.
- By default, the device is disabled from sending traps.
- End

## 5.15.5 Enabling the Trap Function When the Transmission Delay Exceeds the Threshold

### Context

Do as follows on the NQA client.

## Procedure

- Step 1** Run the **system-view?** command to enter the system view.
- Step 2** Run the **nqa test-instance** *admin-name test-name* command to create an NQA test and enter the test instance view.
- Step 3** Run the **send-trap overthreshold** command to enable the trap function.
- By default, the device is disabled from sending traps.
- End

## 5.15.6 Checking the Configuration

### Context

Run the following command to check the previous configuration.

| Action                               | Command                   |
|--------------------------------------|---------------------------|
| Check the traps sent in an NQA test. | <b>display trapbuffer</b> |

## 5.16 Maintaining NQA

This section describes how to maintain NQA.

### Context

#### [5.16.1 Restarting an NQA Test Instance](#)

### [5.16.2 Clearing NQA Statistics](#)

### [5.16.3 Debugging NQA](#)

## 5.16.1 Restarting an NQA Test Instance

### Context



#### CAUTION

Restarting an NQA test instance interrupts the running of tests.

Run the following command in the NQA view to restart an NQA test instance.

| Action                        | Command        |
|-------------------------------|----------------|
| Restart an NQA test instance. | <b>restart</b> |

## 5.16.2 Clearing NQA Statistics

### Context



#### CAUTION

Statistics cannot be restored after being cleared. So, confirm the action before you run the command.

Run the following command in the NQA view to clear NQA statistics.

| Action                                                     | Command              |
|------------------------------------------------------------|----------------------|
| Clear historical statistics on NQA tests and test results. | <b>clear-records</b> |



#### NOTE

Statistics about the running test instance cannot be cleared.

## 5.16.3 Debugging NQA

## Context

When a fault occurs, run the **debugging** command to debug NQA and locate the fault.



### CAUTION

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

| Action                | Command              |
|-----------------------|----------------------|
| Enable NQA debugging. | <b>debugging nqa</b> |

## 5.17 Configuration Examples

This section provides several configuration examples of NQA.

### Context

[5.17.1 Example for Configuring the ICMP Test](#)

[5.17.2 Example for Configuring the DHCP Test](#)

[5.17.3 Example for Configuring an FTP Download Test](#)

[5.17.4 Example for Configuring an FTP Upload Test](#)

[5.17.5 Example for Configuring the HTTP Test](#)

[5.17.6 Example for Configuring the SNMP Query Test](#)

[5.17.7 Example for Configuring a TCP Test](#)

[5.17.8 Example for Configuring the UDP Test](#)

[5.17.9 Example for Configuring a Jitter Test](#)

[5.17.10 Example for Configuring an NQA Test Group](#)

[5.17.11 Example for Enabling the Trap Function When the Transmission Delay Exceeds the Threshold](#)

### 5.17.1 Example for Configuring the ICMP Test

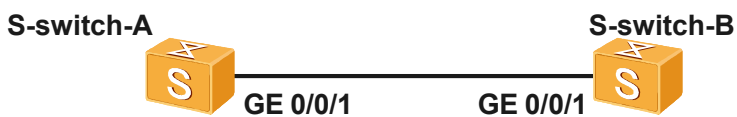
#### Context

#### Networking Requirements

As shown in [Figure 5-3](#),

S-switch-A functions as an NQA client. It is required to test whether S-switch-B is reachable.

**Figure 5-3** Networking diagram of the ICMP test



## Configuration Roadmap

The configuration roadmap is as follows:

1. Perform the NQA ICMP test to test whether S-switch-A and S-switch-B are reachable and to obtain the RTT of a packet.

## Data Preparation

To complete the configuration, you need the following data:

- IP address of S-switch-B

## Configuration Procedure

1. Complete the following configurations to ensure that S-switch-A and S-switch-B are reachable. (The detailed procedure is not mentioned here.)

Create VLAN 1 on S-switch-A and S-switch-B

Add interfaces connecting S-switch-A with S-switch-B to VLAN 1.

Configure the IP address of VLANIF 1 on S-switch-A and S-switch-B.

2. Enable the NQA client and create an NQA ICMP test.

```

<S-switch-A> system-view
[S-switch-A] nqa test-instance admin icmp
[S-switch-A-nqa-admin-icmp] test-type icmp
[S-switch-A-nqa-admin-icmp] destination-address ipv4 10.1.1.2

```

3. Perform the test immediately.

```

[S-switch-A-nqa-admin-icmp] start now

```

4. Verify the configuration.

```

[S-switch-A-nqa-admin-icmp] display nqa results admin icmp
NQA entry(admin, icmp) :testFlag is inactive ,testtype is icmp
 1 . Test 1 result The test is finished
 Send operation times :3 Receive response times :3
 Completion :success RTD OverThresholds number:0
 Attempts number :1 Drop operation number :0
 Disconnect operation number :0 Operation timeout number :0
 System busy operation number :0 Connection fail number :0
 Operation sequence errors number:0 RTT Stats errors number :0
 Destination ip address :10.1.1.2
 Min/Max/Average Completion Time :1/1/1
 Sum/Square-Sum Completion Time :3/3
 Last Good Probe Time :2008-1-1 0:21:35.3

```

## Configuration Files

- Configuration file of S-switch-A

```

#
sysname S-switch-A
vlan batch 1
.....

```

```

interface Vlanif1
ip address 10.1.1.1 255.255.255.0
interface Ethernet0/0/1
port default vlan 1
.....
nqa test-instance admin icmp
test-type icmp
destination-address ipv4 10.1.1.2
#
.....

```

- Configuration file of S-switch-B

```

#
S-switch-B
vlan batch 1
.....
interface Vlanif1
interface Ethernet0/0/1
port default vlan 1
ip address 10.1.1.2 255.255.255.0
.....

```

## 5.17.2 Example for Configuring the DHCP Test

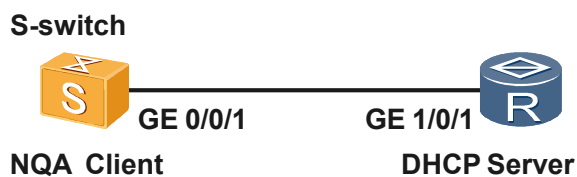
### Context

### Networking Requirements

It is required to meet the following conditions, as shown in [Figure 5-4](#):

- The router functions as the DHCP server.
- An NQA DHCP test is performed to obtain the time during which the DHCP server assigns an IP address to the NQA client.

**Figure 5-4** Networking diagram of the DHCP test



### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the S-switch as the NQA client.
2. Create and perform the DHCP test on the S-switch to check whether the S-switch can set up a connection with and obtain an IP address from the DHCP server.

### Data Preparation

To complete the configuration, you need the following data:

- IP address of the DHCP server

- Source interface
- Timeout period

## Configuration Procedure

1. Complete the configuration of the DHCP server to ensure that the S-switch and the router are reachable. The details about the configuration are not mentioned here.
2. Enable the NQA client and create an NQA DHCP test.

```
<S-switch> system-view
[S-switch] nqa test-instance admin dhcp
[S-switch-nqa-admin-dhcp] test-type dhcp
[S-switch-nqa-admin-dhcp] source-interface ethernet 0/0/10
[S-switch-nqa-admin-dhcp] timeout 20
```

3. Perform the test.

```
[S-switch-nqa-admin-dhcp] start now
```

4. Verify the configuration.

```
[S-switch-nqa-admin-dhcp] display nqa results admin dhcp
NQA entry(admin, dhcp) :testFlag is inactive ,testtype is dhcp
1 .Test 1 result The test is finished
 Send operation times: 3 Receive response times: 1
 Completion:success RTD OverThresholds number: 0
 Attempts number:1 Drop operation number:0
 Disconnect operation number:0 Operation timeout number:2
 System busy operation number:0 Connection fail number:0
 Operation sequence errors number:0 RTT Stats errors number:0
 Destination ip address:10.1.1.3
 Min/Max/Average Completion Time: 1030/1030/1030
 Sum/Square-Sum Completion Time: 1030/1060900
 Last Good Probe Time: 2008-9-27 16:00:2.2
```

## Configuration Files

- Configuration file of the S-switch

```
#
sysname S-switch
vlan batch 1
....
interface Vlanif1
ip address 10.1.1.1 255.255.255.0
interface Ethernet0/0/1
port default vlan 1
....
nqa test-instance admin dhcp
 test-type dhcp
 timeout 20
 source-interface Ethernet 0/0/10
#
.....
```

## 5.17.3 Example for Configuring an FTP Download Test

### Context

### Networking Requirements

As shown in [Figure 5-5](#),

- S-switch-B functions as the FTP server.
- It is required to log in to the FTP server with a user name of **user1** and a password of **hello** and to specify the file to be downloaded as **test.txt**.

**Figure 5-5** Networking diagram of the FTP test



## Configuration Roadmap

To complete the configuration, you need to perform the following operations:

1. Configure S-switch-A as the NQA client.
2. Create and perform the FTP test on S-switch-A to check whether it can set up a connection with the specified FTP server and obtain the time S-switch-A takes to download a file from the FTP server.

## Data Preparation

To complete the configuration, you need the following data:

- IP address of the FTP server
- Source IP address for the test
- FTP user name and password
- Operation file of the FTP test

## Configuration Procedure

1. Complete the following configurations to ensure that S-switch-A and S-switch-B are reachable. (The detailed procedure is not mentioned here.)

Create VLAN 1 on S-switch-A and S-switch-B

Add interfaces connecting S-switch-A with S-switch-B to VLAN 1.

Configure the IP address of VLANIF 1 on S-switch-A and S-switch-B.

2. Configure S-switch-B as the FTP server.

```

<S-switch-B> system-view
[S-switch-B] ftp server enable
[S-switch-B] aaa
[S-switch-B-aaa] local-user user1 password cipher hello
[S-switch-B-aaa] local-user user1 service-type ftp
[S-switch-B-aaa] local-user user1 ftp-directory flash:/
[S-switch-B-aaa] quit

```

3. Create an NQA FTP test on S-switch-A.

```

<S-switch-A> system-view
[S-switch-A] nqa test-instance admin ftp
[S-switch-A-nqa-admin-ftp] test-type ftp
[S-switch-A-nqa-admin-ftp] destination-address ipv4 10.1.1.2
[S-switch-A-nqa-admin-ftp] source-address ipv4 10.1.1.1

```

- ```
[S-switch-A-nqa-admin-ftp] ftp-operation get
[S-switch-A-nqa-admin-ftp] ftp-username user1
[S-switch-A-nqa-admin-ftp] ftp-password hello
[S-switch-A-nqa-admin-ftp] ftp-filename test.txt
```
4. Perform the test.

```
[S-switch-A-nqa-admin-ftp] start now
```
 5. Verify the configuration.

```
[S-switch-A-nqa-admin-ftp] display nqa results admin ftp
NQA entry(admin, ftp) :testFlag is inactive ,testtype is ftp
 1 . Test 1 result The test is finished
    SendProbe:1                                ResponseProb:1
    Completion :success                        RTD OverThresholds number: 0
    MessageBodyOctetsSum: 448                  Stats errors number: 0
    Operation timeout number: 0                System busy operation number:0
    Drop operation number:0                    Disconnect operation number: 0
    CtrlConnTime Min/Max/Average: 438/438/438
    DataConnTime Min/Max/Average: 218/218/218
    SumTime Min/Max/Average: 656/656/656
```

Configuration Files

- Configuration files of S-switch-A

```
#
sysname S-switch-A
vlan batch 1
....
interface Vlanif1
ip address 10.1.1.1 255.255.255.0
interface Ethernet0/0/1
port default vlan 1
#
nqa test-instance admin ftp
test-type ftp
destination-address ipv4 10.1.1.2
source-address ipv4 10.1.1.1
ftp-operation get
ftp-filename test.txt
ftp-username user1
ftp-password hello
....
return
```

- Configuration files of S-switch-B

```
#
sysname S-switch-B
vlan batch 1
....
FTP server enable
#
interface Vlanif1
ip address 10.1.1.2 255.255.255.0
interface Ethernet0/0/1
port default vlan 1
....
aaa
local-user user1 password cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
local-user user1 service-type ftp
local-user user1 ftp-directory flash:/
....
```

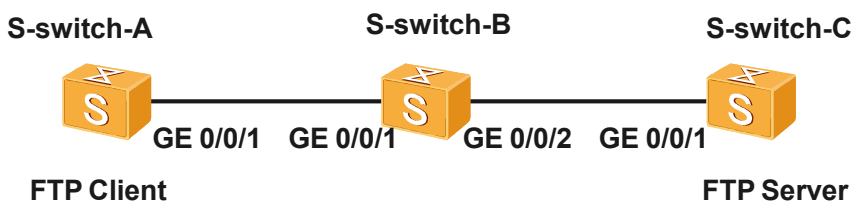
5.17.4 Example for Configuring an FTP Upload Test

Context

Networking Requirements

As shown in [Figure 5-6](#),
it is required to test the speed of uploading a file to the FTP server (S-switch-C).

Figure 5-6 Networking diagram of the FTP test



Configuration Roadmap

The configuration roadmap is follows:

1. Configure S-switch-A as the NQA client and FTP client. Create and perform the FTP test on S-switch-A to check whether it can set up a connection with the specified FTP server and obtain the time taken to upload a file to the FTP server.
2. Specify the user name and password of the FTP server as **user1** and **hello** respectively to log in to the FTP server, and upload a 10 KB file.

Data Preparation

To complete the configuration, you need the following data:

- IP address of the FTP server
- Source IP address of the FTP client that is performing the test
- FTP user name and password
- Size of the uploaded file through FTP

Configuration Procedure

1. Complete the following configurations to ensure that S-switch-A and S-switch-B are reachable. (The detailed procedure is not mentioned here.)
Create VLAN 1 on S-switch-A, VLAN 1 and VLAN 2 on S-switch-B, and VLAN 2 on S-switch-C.
Add physical interfaces connecting S-switch-A with S-switch-B to VLAN 1 and add interfaces connecting S-switch-B with S-switch-C to VLAN 2.
Configure the IP address of VLANIF 1 on S-switch-A, the IP addresses of VLANIF 1 and VLANIF 2 on S-switch-B, and the IP address of VLANIF 2 on S-switch-C.
Configure the route to S-switch-C on S-switch-A and configure the route to S-switch-A on S-switch-C.
2. Configure S-switch-C as the FTP server.

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

```
[S-switch-C] ftp server enable
[S-switch-C] aaa
[S-switch-C-aaa] local-user user1 password cipher hello
[S-switch-C-aaa] local-user user1 service-type ftp
[S-switch-C-aaa] local-user user1 ftp-directory flash:
[S-switch-C-aaa] quit
```

3. Create an NQA FTP test on S-switch-A and create a 10 KB file named **nqa-ftp-test.txt** for uploading.

```
<S-switch-A> system-view
[S-switch-A] nqa test-instance admin ftp
[S-switch-A-nqa-admin-ftp] test-type ftp
[S-switch-A-nqa-admin-ftp] destination-address ipv4 10.2.1.2
[S-switch-A-nqa-admin-ftp] source-address ipv4 10.1.1.1
[S-switch-A-nqa-admin-ftp] ftp-operation put
[S-switch-A-nqa-admin-ftp] ftp-username user1
[S-switch-A-nqa-admin-ftp] ftp-password hello
[S-switch-A-nqa-admin-ftp] ftp-filesize 10
```

4. Perform the test.

```
[S-switch-A-nqa-admin-ftp] start now
```

5. Verify the configuration.

View the test results on S-switch-A.

```
[S-switch-A-nqa-admin-ftp] display nqa results admin ftp
NQA entry(admin, ftp) :testFlag is inactive ,testtype is ftp
 1 . Test 1 result The test is finished
  SendProbe:1 ResponseProbe:1
  Completion :success RTD OverThresholds number: 0
  MessageBodyOctetsSum: 10240 Stats errors number: 0
  Operation timeout number: 0 System busy operation number:0
  Drop operation number:0 Disconnect operation number: 0
  CtrlConnTime Min/Max/Average: 70/70/70
  DataConnTime Min/Max/Average: 2580/2580/2580
  SumTime Min/Max/Average: 2650/2650/2650
```

You can view a file named **nqa-ftp-test.txt** is added on S-switch-C.

```
<S-switch-C> dir
Directory of flash:/
 0 -rw- 331 Jul 06 2007 18:34:34 private-data.txt
 1 -rw- 10240 Jul 06 2007 18:37:06 nqa-ftp-test.txt
2540 KB total (1536 KB free)
```

Configuration Files

- Configuration files of S-switch-A

```
#
 sysname S-switch-A
 vlan batch 1
 ....
 interface Vlanif1
 ip address 10.1.1.1 255.255.255.0
 #
 interface Ethernet0/0/1
 port default vlan 1
 ....
 nqa test-instance admin ftp
 test-type ftp
 destination-address ipv4 10.2.1.2
 source-address ipv4 10.1.1.1
 ftp-operation put
 ftp-filesize 10
 ftp-username user1
 ftp-password hello
 ....
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
 #
```

- ```

....

```
- Configuration files of S-switch-B
 

```

#
sysname S-switch-B
vlan batch 1 2
....
interface Vlanif1
ip address 10.1.1.2 255.255.255.0
#
ip address 10.2.1.1 255.255.255.0
#
interface Ethernet0/0/1
port default vlan 1
interface Ethernet0/0/2
port default vlan 2
interface Vlanif2
....

```
  - Configuration files of S-switch-C
 

```

#
sysname S-switch-C
vlan batch 1
....
FTP server enable
#
interface Vlanif2
ip address 10.2.1.2 255.255.255.0
interface Ethernet0/0/1
port default vlan 2
....
aaa
local-user user1 password cipher 3MQ*TZ,03KCQ=^Q`MAF4<1!!
local-user user1 service-type ftp
local-user user1 ftp-directory flash:
#
ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
....

```

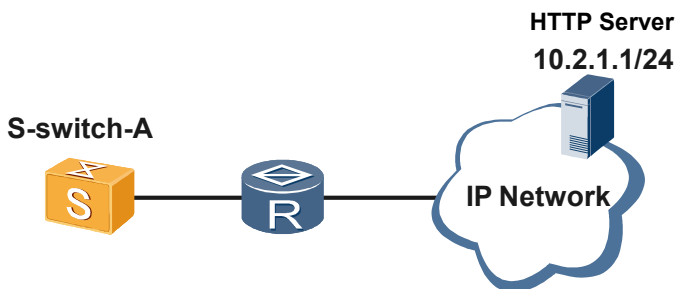
## 5.17.5 Example for Configuring the HTTP Test

### Context

### Networking Requirements

As shown in [Figure 5-7](#), S-switch-A is connected with the HTTP server through a Wide Area Network (WAN).

**Figure 5-7** Networking diagram of the HTTP test



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure S-switch-A as the NQA client.
2. Create and perform the HTTP test on S-switch-A to check whether S-switch-A can set up a connection with the HTTP server and obtain the time taken to transfer a file.

## Data Preparation

To complete the configuration, you need the following data:

- IP address of the HTTP server
- HTTP operation type

## Configuration Procedure

1. Configure the IP address to ensure that the S-switch and the HTTP server are reachable.
2. Enable the NQA client and create an NQA HTTP test.

```
<S-switch-A> system-view
[S-switch-A] nqa test-instance admin http
[S-switch-A-nqa-admin-http] test-type http
[S-switch-A-nqa-admin-http] destination-address ipv4 10.2.1.1
[S-switch-A-nqa-admin-http] http-operation get
[S-switch-A-nqa-admin-http] http-url www.huawei.com
```

3. Perform the test.

```
[S-switch-A-nqa-admin-http] start now
```

4. Verify the configuration.

```
[S-switch-A-nqa-admin-http] display nqa results admin http
NQA entry(admin, http) :testFlag is inactive ,testtype is http
 1 . Test 1 result The test is finished
 SendProbe:3 ResponseProb:3
 Completions: success RTD OverThresholds number: 0
 MessageBodyOctetsSum: 0 TargetAddress: 10.2.1.1
 DNSQueryError number: 0 HTTPError number: 0
 TcpConnError number : 3 System busy operation number:0
 DNSRTT Sum/Min/Max:0/0/0 TCPConnectRTT Sum/Min/Max: 0/0/0
 TransactionRTT Sum/Min/Max: 11/3/4 RTT Sum/Min/Max: 18/5/7
 DNSServerTimeout:0 TCPConnectTimeout:0 TransactionTimeout: 0
```

## Configuration Files

Configuration files of S-switch-A

```
#
sysname S-switch-A
vlan batch 1
....
interface Vlanif1
 ip address 10.1.1.1 255.255.255.0
#
interface Ethernet0/0/1
port default vlan 1
#
nqa test-instance admin http
 test-type http
 destination-address ipv4 10.2.1.1
 http-operation get
 http-url www.huawei.com
#
```

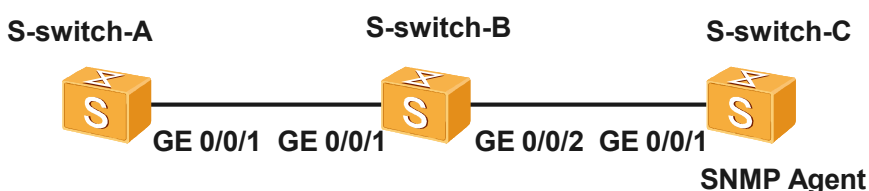
....

## 5.17.6 Example for Configuring the SNMP Query Test

### Networking Requirements

As shown in [Figure 5-8](#), S-switch-C functions as an SNMP agent. It is required to perform an NQA SNMP Query test to obtain the period of time from sending an SNMP query packet to receiving a response packet.

**Figure 5-8** Networking diagram of the SNMP Query test



### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure S-switch-A as an NQA client.
2. Create and perform an SNMP Query test on S-switch-A.
3. Enable SNMP agent on S-switch-C.

### Data Preparation

To complete the configuration, you need the following data.

- IP address of the SNMP agent

### Procedure

**Step 1** Configure S-switch-A, S-switch-B, and S-switch-C to be reachable. (The detailed procedure is not mentioned here.)

**Step 2** Enable SNMP agent on S-switch-C.

```
<S-switch-C> system-view
[S-switch-C] snmp-agent
```

**Step 3** Create an SNMP Query test instance on S-switch-A.

```
<S-switch-A> system-view
[S-switch-A] nqa test-instance admin snmp
[S-switch-A-nqa-admin-snmp] test-type snmp
[S-switch-A-nqa-admin-snmp] destination-address ipv4 10.2.1.2
```

**Step 4** Start the test.

```
[S-switch-A-nqa-admin-snmp] start now
```

**Step 5** View the test results.

```
[S-switch-A-nqa-admin-snmp] display nqa results admin snmp
NQA entry(admin, snmp) :testFlag is inactive ,testtype is snmp
1 . Test 1 result The test is finished
Send operation times: 3 Receive response times: 3
```

```
Completion:success RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:10.2.1.2
Min/Max/Average Completion Time: 10/30/16
Sum/Square-Sum Completion Time: 50/1100
Last Good Probe Time: 2008-8-2 4:13:19.4
```

----End

## Configuration Files

- Configuration file of S-switch-A

```
#
 sysname S-switch-A
vlan batch 1
....
#
interface Vlanif1
 ip address 10.1.1.1 255.255.255.0
interface Ethernet0/0/1
 port default vlan 1
....
nqa test-instance admin snmp
 test-type snmp
 destination-address ipv4 10.2.1.2
....
ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
 ntp-service unicast-server 10.1.1.2
#
....
```

- Configuration file of S-switch-B

```
#
 sysname S-switch-B
vlan batch 1 2
#
interface Vlanif1
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif2
 ip address 10.2.1.1 255.255.255.0
interface Ethernet0/0/1
 port default vlan 1
interface Ethernet0/0/2
 port default vlan 2
....
```

- Configuration file of S-switch-C

```
#
 sysname S-switch-C
vlan batch 2
#
interface Vlanif2
 ip address 10.2.1.2 255.255.255.0
interface Ethernet0/0/1
 port default vlan 2
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
snmp-agent
snmp-agent local-engineid 000007DB7F00000100006294
snmp-agent sys-info version v3
snmp-agent trap queue-size 32
#
```

....

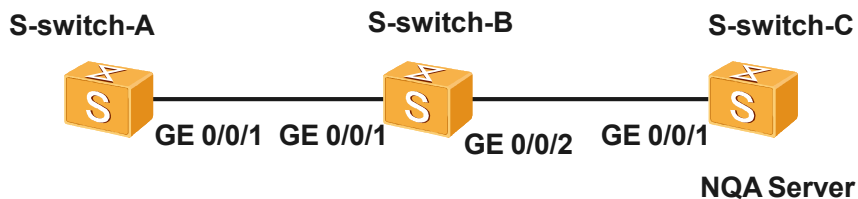
## 5.17.7 Example for Configuring a TCP Test

### Context

### Networking Requirements

As shown in [Figure 5-9](#), the NQA TCP Private test is performed to obtain the time taken for S-switch-A to set up a TCP connection with S-switch-C.

**Figure 5-9** Networking diagram of the TCP test



### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure S-switch-A as the NQA client and configure S-switch-C as the NQA server.
2. Configure the number of the port monitored by the NQA server and create an NQA TCP test on the NQA client.

### Data Preparation

To complete the configuration, you need the following data:

- IP address of the server
- Number of the TCP port monitored by the server

### Configuration Procedure

1. Complete the following configurations to ensure that S-switch-A, S-switch-B and S-switch-C are reachable. (The detailed procedure is not mentioned here.)

Create VLAN 1 on S-switch-A, VLAN 1 and VLAN 2 on S-switch-B, and VLAN 2 on S-switch-C.

Add physical interfaces connecting S-switch-A with S-switch-B to VLAN 1 and add interfaces connecting S-switch-B with S-switch-C to VLAN 2.

Configure the IP address of VLANIF 1 on S-switch-A, the IP addresses of VLANIF 1 and VLANIF 2 on S-switch-B, and the IP address of VLANIF 2 on S-switch-C.

Configure the route to S-switch-C on S-switch-A and configure the route to S-switch-A on S-switch-C.

2. Configure the NQA server on S-switch-C.

# Configure the IP address and interface number monitored by the server.

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

- ```
[S-switch-C] nqa-server tcpconnect 10.2.1.2 9000
```
3. Configure S-switch-A.
Enable the NQA client and create a TCP Private test.

```
<S-switch-A> system-view
[S-switch-A] nqa test-instance admin tcp
[S-switch-A-nqa-admin-tcp] test-type tcp
[S-switch-A-nqa-admin-tcp] destination-address ipv4 10.2.1.2
[S-switch-A-nqa-admin-tcp] destination-port 9000
```
 4. Perform the test.

```
[S-switch-A-nqa-admin-tcp] start now
```
 5. Verify the configuration.

```
[S-switch-A-nqa-admin-tcp] display nqa results admin tcp
NQA entry(admin, tcp) :testFlag is inactive ,testtype is tcp
1 Test 1 result The test is finished
  Send operation times: 3          Receive response times: 3
  Completion:success           RTD OverThresholds number: 0
  Attempts number:1            Drop operation number:0
  Disconnect operation number:0 Operation timeout number:0
  System busy operation number:0 Connection fail number:0
  Operation sequence errors number:0 RTT Stats errors number:0
  Destination ip address:2.1.1.2
  Min/Max/Average Completion Time: 10/10/10
  Sum/Square-Sum Completion Time: 30/300
  Last Good Probe Time: 2008-8-30 14:17:1.5
```

Configuration Files

- Configuration files of S-switch-A

```
#
 sysname S-switch-A
 vlan batch 1
 ....
#
 interface Vlanif1
  ip address 10.1.1.1 255.255.255.0
#
 interface Ethernet0/0/1
 port default vlan 1
 ....
 nqa test-instance admin tcp
  test-type tcp
  destination-address ipv4 10.2.1.2
  destination-port 9000
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
 ....
```

- Configuration files of S-switch-B

```
#
 sysname S-switch-B
 vlan batch 1 2
 ....
#
 interface Vlanif1
  ip address 10.1.1.2 255.255.255.0
#
 interface Vlanif2
  ip address 10.2.1.1 255.255.255.0
#
 interface Ethernet0/0/1
 port default vlan 1
 interface Ethernet0/0/2
 port default vlan 2
```

- Configuration files of S-switch-C


```

      ....
      #
      sysname S-switch-C
      vlan batch 1
      ....
      #
      interface Vlanif2
      ....
      ip address 10.2.1.2 255.255.255.0
      #
      interface Ethernet0/0/1
      port default vlan 2
      #
      nqa-server tcpconnect 10.2.1.2 9000
      #
      ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
      #
      ....
      
```

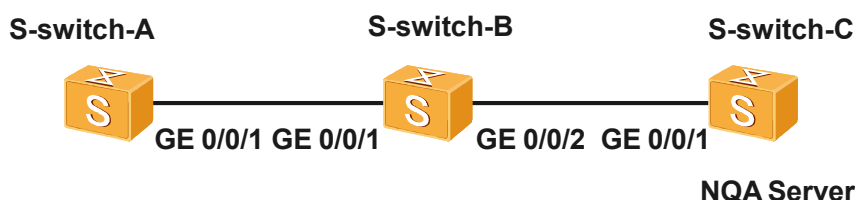
5.17.8 Example for Configuring the UDP Test

Context

Networking Requirements

As shown in [Figure 5-10](#), the NQA UDP Public test is performed to obtain RTT of a UDP packet transmitted between S-switch-A and S-switch-C.

Figure 5-10 Networking diagram of the UDP test



Configuration Roadmap

1. Configure S-switch-A as the NQA client and configure S-switch-C as the NQA server.
2. Configure the interface number monitored by the NQA server and create an NQA UDP Public test on the NQA client.

Data Preparation

To complete the configuration, you need the following data:

- IP address of the NQA server
- Number of the UDP port monitored by the server

Configuration Procedure

1. Complete the following configurations to ensure that S-switch-A, S-switch-B and S-switch-C are reachable. (The detailed procedure is not mentioned here.)

Create VLAN 1 on S-switch-A, VLAN 1 and VLAN 2 on S-switch-B, and VLAN 2 on S-switch-C.

Add physical interfaces connecting S-switch-A with S-switch-B to VLAN 1 and add interfaces connecting S-switch-B with S-switch-C to VLAN 2.

Configure the IP address of VLANIF 1 on S-switch-A, the IP addresses of VLANIF 1 and VLANIF 2 on S-switch-B, and the IP address of VLANIF 2 on S-switch-C.

Configure the route to S-switch-C on S-switch-A and configure the route to S-switch-A on S-switch-C.

2. Configure the NQA server on S-switch-C.

Configure the IP address and UDP interface number monitored by the NQA server.

```
<S-switich-C> system-view
[S-switich-C] nqa-server udpecho 10.2.1.2 6000
```

3. Configure S-switch-A.

Enable the NQA client and create a UDP Public test.

```
<S-switich-A> system-view
[S-switich-A] nqa test-instance admin udp
[S-switich-A-nqa-admin-udp] test-type udp
[S-switich-A-nqa-admin-udp] destination-address ipv4 10.2.1.2
[S-switich-A-nqa-admin-udp] destination-port 6000
```

4. Perform the test.

```
[S-switich-A-nqa-admin-udp] start now
```

5. Verify the configuration.

```
[S-switich-A-nqa-admin-udp] display nqa results admin udp
NQA entry(admin, udp) :testFlag is inactive ,testtype is udp
 1 . Test 1 result The test is finished
    Send operation times: 3          Receive response times: 3
    Completion:success             RTD OverThresholds number: 0
    Attempts number:1              Drop operation number:0
    Disconnect operation number:0   Operation timeout number:0
    System busy operation number:0  Connection fail number:0
    Operation sequence errors number:0 RTT Stats errors number:0
    Destination ip address:2.1.1.2
    Min/Max/Average Completion Time: 1/20/13
    Sum/Square-Sum Completion Time: 41/801
    Last Good Probe Time: 2008-8-30 14:25:44.2
```

Configuration Files

- Configuration files of S-switch-A

```
#
sysname S-switich-A
vlan batch 1
....
#
interface Vlanif1
 ip address 10.1.1.1 255.255.255.0
interface Ethernet0/0/1
port default vlan 1
....
#
nqa test-instance admin udp
 test-type udp
 destination-address ipv4 10.2.1.2
 destination-address port 6000
....
ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
....
```

- Configuration files of S-switch-B

```
#
 sysname S-switich-B
 vlan batch 1 2
 ....
 interface Vlanif1
  ip address 10.1.1.2 255.255.255.0
 #
 interface Vlanif2
  ip address 10.2.1.1 255.255.255.0
 interface Ethernet0/0/1
  port default vlan 1
 interface Ethernet0/0/2
  port default vlan 2
 ....
 #
 ....
```

- Configuration files of S-switch-C

```
#
 sysname S-switich-C
 vlan batch 2
 #
 interface Vlanif2
 ....
  ip address 10.2.1.2 255.255.255.0
 interface Ethernet0/0/1
  port default vlan 2
 #
 nqa-server udpecho 10.2.1.2 6000
 #
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
 #
 ....
```

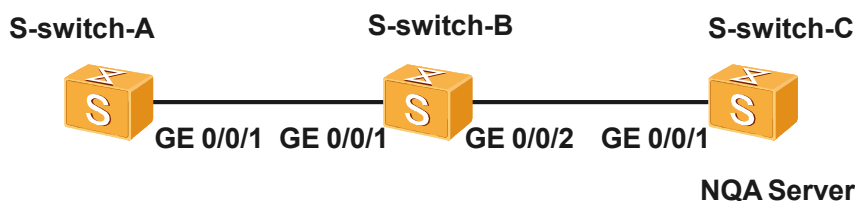
5.17.9 Example for Configuring a Jitter Test

Context

Networking Requirements

As shown in [Figure 5-11](#), the NQA jitter test is performed to obtain the jitter time of transmitting a packet between S-switch-A and S-switch-C.

Figure 5-11 Networking diagram of a jitter test



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure S-switch-A as the Network Time Protocol (NTP) client and configure S-switch-B as the NTP server.

2. Configure S-switch-C as the NTP client and configure S-switch-B as the NTP server.
3. Configure S-switch-A as the NQA client and configure S-switch-C as the NQA server.
4. Configure the service type and the number of the port monitored by the NQA server.
5. Configure an NQA jitter test on the NQA client.

Data Preparation

To complete the configuration, you need the following data:

- IP address of the server
- Number of the UDP port monitored by the server

Configuration Procedure

1. Complete the following configurations to ensure that S-switch-A, S-switch-B and S-switch-C are reachable. (The detailed procedure is not mentioned here.)

Create VLAN 1 on S-switch-A, VLAN 1 and VLAN 2 on S-switch-B, and VLAN 2 on S-switch-C.

Add physical interfaces connecting S-switch-A with S-switch-B to VLAN 1 and add interfaces connecting S-switch-B with S-switch-C to VLAN 2.

Configure the IP address of VLANIF 1 on S-switch-A, the IP addresses of VLANIF 1 and VLANIF 2 on S-switch-B, and the IP address of VLANIF 2 on S-switch-C.

Configure the route to S-switch-C on S-switch-A and configure the route to S-switch-A on S-switch-C.

2. On S-switch-A, specify S-switch-B as its NTP server.

```
<S-switch-A> system-view
[S-switch-A] ntp-service unicast-server 10.1.1.2
```

3. On S-switch-C, specify S-switch-B as its NTP server.

```
<S-switch-C> system-view
[S-switch-C] ntp-service unicast-server 10.2.1.1
```

4. Configure the NQA server on S-switch-C.

Configure the IP address and UDP interface number monitored by the NQA server.

```
<S-switch-C> system-view
[S-switch-C] nqa-server udpecho 10.2.1.2 9000
```

5. Configure S-switch-A.

Enable the NQA client and create an NQA Jitter test.

```
<S-switch-A> system-view
[S-switch-A] nqa test-instance admin jitter
[S-switch-A-nqa-admin-jitter] test-type jitter
[S-switch-A-nqa-admin-jitter] destination-address ipv4 10.2.1.2
[S-switch-A-nqa-admin-jitter] destination-port 9000
```

6. Perform the test.

```
[S-switch-A-nqa-admin-jitter] start now
```

7. Verify the configuration.

```
[S-switch-A-nqa-admin-jitter] display nqa results admin jitter
NQA entry(admin, jitter) :testFlag is inactive ,testtype is jitter
1 . Test 1 result The test is finished
  SendProbe:60                               ResponseProbe:60
  Completion :success                         RTD OverThresholds number:0
  Min/Max/Sum RTT:1/20/199                    RTT Square Sum:2349
  NumOfRTT:60                                Drop operation number:0
```

Operation sequence errors number:0	RTT Stats errors number:0
System busy operation number:0	Operation timeout number:0
Min Positive SD:10	Min Positive DS:10
Max Positive SD:130	Max Positive DS:20
Positive SD Number:13	Positive DS Number:12
Positive SD Sum:420	Positive DS Sum:130
Positive SD Square Sum :36600	Positive DS Square Sum :1500
Min Negative SD:10	Min Negative DS:10
Max Negative SD:20	Max Negative DS:120
Negative SD Number:16	Negative DS Number:13
Negative SD Sum:200	Negative DS Sum:350
Negative SD Square Sum :2800	Negative DS Square Sum :27900
Packet Loss SD:0	Packet Loss DS:0
Max Delay SD:10	Max Delay DS:9
jitter out value:7.8801084	jitter in value:6.2393465
OWD OverThresholds number:0	Packet Loss Unknown:0
NumberOfOWD:60	
OWD SD Sum:75	OWD DS Sum:64

Configuration Files

- Configuration files of S-switch-A

```
#
 sysname S-switch-A
vlan batch 1
....
#
interface Vlanif1
 ip address 10.1.1.1 255.255.255.0
interface Ethernet0/0/1
port default vlan 1
....
nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 10.2.1.2
 destination-port 9000
....
ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
ntp-service unicast-server 10.1.1.2
#
....
```

- Configuration files of S-switch-B

```
#
 sysname S-switch-B
vlan batch 1 2
#
interface Vlanif1
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif2
 ip address 10.2.1.1 255.255.255.0
interface Ethernet0/0/1
port default vlan 1
interface Ethernet0/0/2
port default vlan 2
....
```

- Configuration files of S-switch-C

```
#
 sysname S-switch-C
vlan batch 2
#
interface Vlanif2
 ip address 10.2.1.2 255.255.255.0
interface Ethernet0/0/1
port default vlan 2
```

```
#
 nqa-server udpecho 10.2.1.2 9000
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
 ntp-service unicast-server 10.2.1.1
#
....
```

5.17.10 Example for Configuring an NQA Test Group

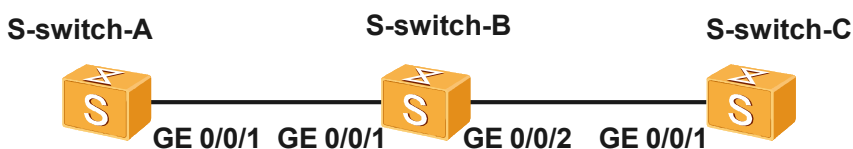
Context

Networking Requirements

As shown in [Figure 5-12](#),

S-switch-A functions as an NQA client. It is required to test whether S-switch-B and S-switch-C are reachable.

Figure 5-12 Networking diagram of an NQA test group



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure S-switch-A as the NQA client.
2. On S-switch-A, create an NQA test group that consists of two test members named **admin test1** and **admin test2** to check whether S-switch-B and S-switch-C are reachable and check the RTT of a test packet.

Data Preparation

To complete the configuration, you need the following data:

- IP addresses of S-switch-B and S-switch-C
- Time when the test group is enabled

Configuration Procedure

1. Complete the following configurations to ensure that S-switch-A, S-switch-B and S-switch-C are reachable. (The detailed procedure is not mentioned here.)

Create VLAN 1 on S-switch-A, VLAN 1 and VLAN 2 on S-switch-B, and VLAN 2 on S-switch-C.

Add physical interfaces connecting S-switch-A with S-switch-B to VLAN 1 and add interfaces connecting S-switch-B with S-switch-C to VLAN 2.

Configure the IP address of VLANIF 1 on S-switch-A, the IP addresses of VLANIF 1 and VLANIF 2 on S-switch-B, and the IP address of VLANIF 2 on S-switch-C.

Configure the route to S-switch-C on S-switch-A and configure the route to S-switch-A on S-switch-C.

2. Create an ICMP test on S-switch-A.

```
<S-switch-A> system-view
[S-switch-A] nqa test-instance group icmp
[S-switch-A-nqa-group-icmp] test-type icmp
[S-switch-A-nqa-group-icmp] switch-to group
[S-switch-A-nqa-group-icmp] quit
```

3. On S-switch-A, create two test members named **admin test1** and **admin test2**.

```
[S-switch-A] nqa test-instance admin test1
[S-switch-A-nqa-admin-test1] test-type icmp
[S-switch-A-nqa-admin-test1] join group nqa group icmp
[S-switch-A-nqa-admin-test1] destination-address ipv4 10.1.1.2
[S-switch-A-nqa-admin-test1] quit
[S-switch-A] nqa test-instance admin test2
[S-switch-A-nqa-admin-test2] test-type icmp
[S-switch-A-nqa-admin-test2] join group nqa group icmp
[S-switch-A-nqa-admin-test2] destination-address ipv4 10.2.1.2
[S-switch-A-nqa-admin-test2] quit
```

4. Return to the test group view, and set the test to be performed after 10 seconds.

```
[S-switch-A] nqa test-instance group icmp
[S-switch-A-nqa-group-icmp] start delay seconds 10
```

Run the **display nqa-agent** command to view the status of the test group and the test members on the client.

```
[S-switch-A-nqa-group-icmp] display nqa-agent
NQA Tests Max:2000                      NQA Tests Num:3
  NQA Concurrent Requests Max:1000      NQA Concurrent Requests Num:0
  NQA Jitter Concurrent Max:5           NQA Jitter Concurrent Num:0
  NQA icmp Concurrent Max:50           NQA icmp Concurrent Num:0
  NQA Trace Concurrent Max:50          NQA Trace Concurrent Num:0

1  NQA entry(admin, test1):
   test type:icmp                      current flag:inactive
   current status:finished              current completion:succes
   start at : no start time            end at : no end time
   nqa status : group member, belong to group : group icmp

2  NQA entry(admin, test2):
   test type:icmp                      current flag:inactive
   current status:finished              current completion:succes
   start at : no start time            end at : no end time
   nqa status : group member, belong to group : group icmp

3  NQA entry(group, icmp):
   test type:icmp                      current flag:inactive
   current status:finished              current completion:NA
   start at : no start time            end at : no end time
   nqa status : group leader, group members number : 2
```

5. Verify the test result in 20s.

```
[S-switch-A-nqa-admin-icmp] display nqa results
NQA entry(admin, test2) :testFlag is inactive ,testtype is icmp
1 . Test 1 result The test is finished
  Send operation times: 3                Receive response times: 3
  Completion:succes                      RTD OverThresholds number: 0
  Attempts number:1                     Drop operation number:0
  Disconnect operation number:0          Operation timeout number:0
  System busy operation number:0        Connection fail number:0
  Operation sequence errors number:0    RTT Stats errors number:0
  Destination ip address:2.1.1.2
  Min/Max/Average Completion Time: 1/10/4
```

```
Sum/Square-Sum Completion Time: 12/102
Last Good Probe Time: 2008-8-30 15:3:35.3
2 . Test 2 result The test is finished
Send operation times: 3          Receive response times: 3
Completion:success              RTD OverThresholds number: 0
Attempts number:1              Drop operation number:0
Disconnect operation number:0   Operation timeout number:0
System busy operation number:0  Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:2.1.1.2
Min/Max/Average Completion Time: 1/10/4
Sum/Square-Sum Completion Time: 12/102
Last Good Probe Time: 2008-8-30 15:5:34.6
```

Configuration Files

- Configuration files of S-switch-A

```
#
sysname S-switich-A
vlan batch 1
....
#
interface Vlanif1
ip address 10.1.1.1 255.255.255.0
#
interface Ethernet0/0/1
port default vlan 1
....
#
nqa test-instance group icmp
switch-to group
test-type icmp
nqa test-instance admin test1
test-type icmp
join group nqa group icmp
destination-address ipv4 10.1.1.2
nqa test-instance admin test2
test-type icmp
join group nqa group icmp
destination-address ipv4 10.2.1.2
#
ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
....
```

- Configuration files of S-switch-B

```
#
sysname S-switich-B
vlan batch 1 2
....
#
interface Vlanif1
ip address 10.1.1.2 255.255.255.0
#
interface Vlanif2
ip address 10.2.1.1 255.255.255.0
#
interface Ethernet0/0/1
port default vlan 1
interface Ethernet0/0/2
port default vlan 2
....
#
....
```

- Configuration files of S-switch-C

```
#
sysname S-switich-C
```

```

vlan batch 2
....
#
interface Vlanif2
 ip address 10.2.1.2 255.255.255.0
#
interface Ethernet0/0/1
 port default vlan 2
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
....

```

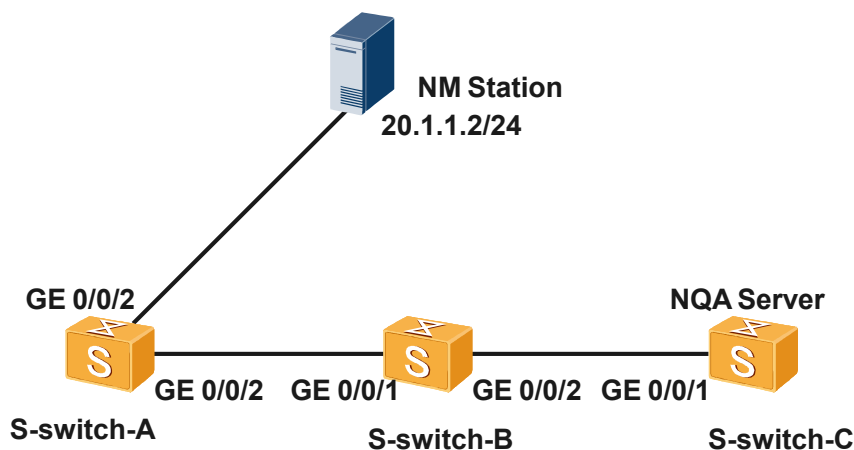
5.17.11 Example for Enabling the Trap Function When the Transmission Delay Exceeds the Threshold

Context

Networking Requirements

Configure a transmission delay threshold and enable the trap function as shown in [Figure 5-13](#). After the jitter test is complete, if the test result shows that the delay of some test packets from S-switch-A to S-switch-C (or from S-switch-C to S-switch-A) exceeds the uni-directional transmission delay, or the bi-directional transmission delay threshold, S-switch-A sends a trap to the NMS. Based on the received trap, the network administrator can clearly find the cause of the fault.

Figure 5-13 Networking diagram of enabling the trap function when the transmission delay exceeds the threshold



NOTE

Configuration Roadmap

The configuration roadmap is as follows:

1. Set a transmission delay threshold.
2. Enable the trap function.

3. Enable the function of sending traps to the NMS.

Data Preparation

To complete the configuration, you need the following data:

- IP address of the NQA server and the port number
- Type of monitoring service and the number of the port monitored by the server
- RTD threshold and OWD threshold
- IP address of the NMS

Configuration Procedure

1. Complete the following configurations to ensure that S-switch-A, S-switch-B and S-switch-C are reachable. (The detailed procedure is not mentioned here.)

Create VLAN 1 and VLAN 2 on S-switch-A, VLAN 2 and VLAN 3 on S-switch-B, and VLAN 3 on S-switch-C.

Add physical interfaces connecting S-switch-A with S-switch-B to VLAN 2 and add interfaces connecting S-switch-B with S-switch-C to VLAN 3.

Configure the IP address of VLANIF 1 and VLANIF 2 on S-switch-A, the IP addresses of VLANIF 2 and VLANIF 3 on S-switch-B, and the IP address of VLANIF 3 on S-switch-C.

Configure Open Shortest Path First (OSPF) on S-switch-A, S-switch-B, and S-switch-C.

2. Configure a Jitter test.

Configure the IP address and the number of the UDP port monitored by the NQA server.

```
<S-switich-C> system-view  
[S-switich-C] nqa-server udpecho 30.1.1.2 9000
```

Enable the NQA client and create an NQA jitter test on S-switich-A.

```
<S-switich-A> system-view  
[S-switich-A] nqa test-instance admin jitter  
[S-switich-A-nqa-admin-jitter] test-type jitter  
[S-switich-A-nqa-admin-jitter] destination-address ipv4 30.1.1.2  
[S-switich-A-nqa-admin-jitter] destination-port 9000
```

3. Set a transmission delay threshold.

Configure the RTD threshold on S-switich-A.

```
[S-switich-A-nqa-admin-jitter] threshold rtd 20
```

Configure the OWD threshold on S-switich-A.

```
[S-switich-A-nqa-admin-jitter] threshold owd 100
```

4. Enable the trap function.

```
[S-switich-A-nqa-test-jitter] send-trap overthreshold  
[S-switich-A-nqa-test-jitter] quit
```

5. Enable the function of sending traps to the NMS.

```
[S-switich-A] snmp-agent trap enable  
[S-switich-A] snmp-agent target-host trap address udp-domain 20.1.1.2 params  
securityname public v2c
```

6. Perform the test.

```
[S-switich-A] nqa test-instance admin jitter  
[S-switich-A-nqa-admin-jitter] start now  
[S-switich-A-nqa-admin-jitter] quit  
[S-switich-A] quit
```

7. Verify the configuration.

View the NQA test results.

```
<S-sw1ch-A> display nqa result
1 . Test 1 result The test is finished
  SendProbe:60                               ResponseProbe:60
  Completion :success                         RTD OverThresholds number:2
  Min/Max/Sum RTT:1/90/479                    RTT Square Sum:15929
  NumOfRTT:60                                Drop operation number:0
  Operation sequence errors number:0          RTT Stats errors number:0
  System busy operation number:0             Operation timeout number:0
  Min Positive SD:10                          Min Positive DS:10
  Max Positive SD:10                          Max Positive DS:10
  Positive SD Number:2                       Positive DS Number:11
  Positive SD Sum:20                          Positive DS Sum:110
  Positive SD Square Sum :200                 Positive DS Square Sum :1100
  Min Negative SD:10                         Min Negative DS:10
  Max Negative SD:20                         Max Negative DS:60
  Negative SD Number:2                      Negative DS Number:14
  Negative SD Sum:30                         Negative DS Sum:190
  Negative SD Square Sum :500                 Negative DS Square Sum :4900
  Packet Loss SD:0                           Packet Loss DS:0
  Max Delay SD:45                             Max Delay DS:44
  jitter out value:0.6854999                  jitter in value:3.8837922
  OWD OverThresholds number:0                 Packet Loss Unknown:0
  NumberOfOWD:60
  OWD SD Sum:225                             OWD DS Sum:194
```

Check whether traps are generated in the trap buffer.

```
<Quidway> display trapbuffer
#Jul  9 00:28:34 2009 Quidway NQA/4/RTDTHRESHOLD:OID
1.3.6.1.4.1.2011.5.25.111.6.16
NQA entry RTD over threshold. (OwnerIndex=admin, TestName=jitter)
#Jul  9 00:28:34 2009 Quidway NQA/4/SDTHRESHOLD:OID
1.3.6.1.4.1.2011.5.25.111.6.17
NQA entry OWD-SD over threshold. (OwnerIndex=admin, TestName=jitter)
#Jul  9 00:28:34 2009 Quidway NQA/4/DSTHRESHOLD:OID
1.3.6.1.4.1.2011.5.25.111.6.18
NQA entry OWD-DS over threshold. (OwnerIndex=admin, TestName=jitter)
```

Check whether the NMS can correctly receive traps. (The detailed configurations are not mentioned here.)

Configuration Files

• Configuration files of S-switch-A

```
#
sysname S-sw1ch-A
#
interface Vlanif1
ip address 10.1.1.1 255.255.255.0
#
interface Vlanif2
ip address 20.1.1.1 255.255.255.0
#
interface Ethernet0/0/1
port default vlan 1
interface Ethernet0/0/2
port default vlan 2
#
nqa test-instance test jitter
test-type jitter
destination-address ipv4 30.1.1.2
destination-port 9000
threshold rtd 20
threshold owd 100
send-trap overthreshold
```

- ```
.....
```
- Configuration files of S-switch-B

```
#
 sysname S-switich-B
vlan batch 2 3
....
interface Vlanif2
#
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif3
 ip address 30.1.1.1 255.255.255.0
#
interface Ethernet0/0/1
port default vlan 2
interface Ethernet0/0/2
port default vlan 3
.....
return
```
  - Configuration files of S-switch-C

```
#
 sysname S-switich-C
vlan batch 3
#
....
interface Vlanif3
 ip address 30.1.1.2 255.255.255.0
#
 nqa-server udpecho 30.1.1.2 9000
#
.....
.....
```