

HP 5120 EI Switch Series

Network Management and Monitoring Configuration Guide

Part number: 5998-1797

Software version: Release 2220

Document version: 6W100-20130810



Legal and notice information

© Copyright 2013 Hewlett-Packard Development Company, L.P.

No part of this documentation may be reproduced or transmitted in any form or by any means without prior written consent of Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

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

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

Contents

Using ping, tracer, and system debugging	1
Ping	1
Using a ping command to test network connectivity	1
Ping example	1
Tracer	3
Prerequisites	4
Using a tracer command to identify failed or all nodes in a path	5
System debugging	5
Debugging information control switches	5
Debugging a feature module	6
Ping and tracer example	7
Configuring NTP	9
Overview	9
NTP application	9
NTP advantages	9
How NTP works	9
NTP message format	10
Operation modes	12
NTP configuration task list	14
Configuring NTP operation modes	14
Configuring the client/server mode	15
Configuring the symmetric peers mode	15
Configuring the broadcast mode	16
Configuring the multicast mode	17
Configuring optional parameters	17
Specifying the source interface for NTP messages	17
Disabling an interface from receiving NTP messages	18
Configuring the allowed maximum number of dynamic sessions	18
Configuring the DSCP value for NTP messages	19
Configuring access-control rights	19
Configuration prerequisites	20
Configuration procedure	20
Configuring NTP authentication	20
Configuring NTP authentication in client/server mode	20
Displaying and maintaining NTP	21
NTP configuration examples	22
Configuring the client/server mode	22
Configuring the NTP symmetric mode	23
Configuring NTP broadcast mode	25
Configuring NTP multicast mode	26
Configuring NTP client/server mode with authentication	29
Configuring NTP broadcast mode with authentication	30
Configuring the information center	34
Overview	34
Classification of system information	35
System information levels	35
Output channels and destinations	35
Outputting system information by source module	36

Default output rules of system information	36
System information formats	37
FIPS compliance	40
Information center configuration task list	40
Outputting system information to the console	40
Outputting system information to the monitor terminal	41
Outputting system information to a log host	42
Outputting system information to the trap buffer	43
Outputting system information to the log buffer	44
Outputting system information to the SNMP module	44
Outputting system information to the Web interface	45
Managing security logs and the security log file	46
Saving security logs into the security log file	46
Managing the security log file	47
Enabling synchronous information output	49
Disabling an interface from generating link up or link down logging information	49
Enabling log file overwrite-protection	50
Displaying and maintaining information center	50
Information center configuration examples	51
Outputting log information to a UNIX log host	51
Outputting log information to a Linux log host	52
Outputting log information to the console	53
Saving security logs into the security log file	54
Configuring SNMP	57
Overview	57
SNMP framework	57
MIB and view-based MIB access control	57
SNMP operations	58
SNMP protocol versions	58
SNMP configuration task list	58
Configuring SNMP basic parameters	58
Configuring SNMPv3 basic parameters	58
Configuring SNMPv1 or SNMPv2c basic parameters	60
Switching the NM-specific interface index format	62
Configuration guidelines	62
Configuration procedure	62
Configuring SNMP logging	63
Configuring SNMP traps	63
Enabling SNMP traps	63
Configuring the SNMP agent to send traps to a host	64
Displaying and maintaining SNMP	65
SNMP configuration examples	66
SNMPv1/SNMPv2c configuration example	66
SNMPv3 configuration example	67
SNMP logging configuration example	69
Configuring RMON	71
Overview	71
Working mechanism	71
RMON groups	71
Configuring the RMON statistics function	73
Configuring the RMON Ethernet statistics function	73
Configuring the RMON history statistics function	73
Configuring the RMON alarm function	74

Displaying and maintaining RMON	75
Ethernet statistics group configuration example	76
History group configuration example	76
Alarm group configuration example	78
Configuring port mirroring	81
Introduction to port mirroring	81
Terminologies of port mirroring	81
Port mirroring classification and implementation	82
Configuring local port mirroring	84
Local port mirroring configuration task list	84
Creating a local mirroring group	84
Configuring source ports for the local mirroring group	84
Configuring the monitor port for the local mirroring group	85
Using the remote probe VLAN to enable local mirroring to support multiple monitor ports	86
Configuring Layer 2 remote port mirroring	87
Layer 2 remote port mirroring configuration task list	87
Configuring a remote destination group (on the destination device)	88
Configuring a remote source group (on the source device)	90
Displaying and maintaining port mirroring	92
Port mirroring configuration examples	92
Local port mirroring configuration example	92
Local port mirroring with multiple monitor ports configuration example	94
Layer 2 remote port mirroring configuration example	95
Configuring traffic mirroring	98
Introduction to traffic mirroring	98
Traffic mirroring configuration task list	98
Configuring match criteria	98
Configuring traffic mirroring of different types	99
Mirroring traffic to a port	99
Mirroring traffic to the CPU	99
Configuring a QoS policy	99
Applying a QoS policy	100
Apply a QoS policy to a port	100
Apply a QoS policy to a VLAN	100
Apply a QoS policy globally	100
Apply a QoS policy to the control plane	101
Displaying and maintaining traffic mirroring	101
Traffic mirroring configuration example	101
Traffic mirroring configuration example	101
Configuring NQA	104
Overview	104
NQA features	104
NQA concepts	106
NQA probe operation procedure	107
NQA configuration task list	107
Configuring the NQA server	108
Enabling the NQA client	108
Creating an NQA test group	109
Configuring an NQA test group	109
Configuring ICMP echo tests	109
Configuring DHCP tests	110
Configuring DNS tests	111
Configuring FTP tests	111

Configuring HTTP tests	113
Configuring UDP jitter tests	113
Configuring SNMP tests	115
Configuring TCP tests	116
Configuring UDP echo tests	117
Configuring voice tests	117
Configuring DLSw tests	119
Configuring the collaboration function	120
Configuring threshold monitoring	121
Configuration prerequisites	121
Configuration guidelines	121
Configuration procedure	121
Configuring the NQA statistics collection function	123
Configuring the history records saving function	123
Configuring optional parameters for an NQA test group	124
Configuring a schedule for an NQA test group	125
Configuration prerequisites	125
Configuration guidelines	126
Configuration procedure	126
Displaying and maintaining NQA	126
NQA configuration examples	127
ICMP echo test configuration example	127
DHCP test configuration example	128
DNS test configuration example	130
FTP test configuration example	131
HTTP test configuration example	132
UDP jitter test configuration example	133
SNMP test configuration example	136
TCP test configuration example	137
UDP echo test configuration example	138
Voice test configuration example	140
DLSw test configuration example	142
NQA collaboration configuration example	143
Configuring sFlow	146
sFlow configuration task list	146
Configuring the sFlow agent and sFlow collector	147
Configuring flow sampling	147
Configuring counter sampling	148
Displaying and maintaining sFlow	148
sFlow configuration example	148
Network requirements	148
Configuration procedure	149
Troubleshooting sFlow configuration	150
Symptom	150
Analysis	150
Solution	150
Configuring IPC	151
Overview	151
Node	151
Link	151
Channel	151
Packet sending modes	152
Enabling IPC performance statistics	152

Displaying and maintaining IPC.....	153
Configuring PoE	154
Overview.....	154
PoE configuration task list	154
Configuration guidelines	155
Enabling PoE for a PoE interface.....	155
Detecting PDs.....	156
Enabling the PSE to detect nonstandard PDs	156
Configuring a PD disconnection detection mode	156
Configuring the maximum PoE interface power	157
Configuring PoE interface power management.....	157
Configuring the PoE monitoring function.....	158
Configuring PSE power monitoring.....	158
Monitoring PD.....	158
Configuring PoE interface through PoE profile	159
Configuring PoE profile	159
Applying a PoE profile.....	159
Upgrading PSE processing software in service	160
Displaying and maintaining PoE	160
PoE configuration example	161
Troubleshooting PoE	162
Setting the priority of a PoE interface to critical fails.....	162
Failure to apply a PoE profile to a PoE interface.....	162
Configuring cluster management	164
Overview.....	164
Roles in a cluster.....	164
How a cluster works.....	165
Configuration restrictions and guidelines.....	168
Cluster management configuration task list.....	168
Configuring the management switch	169
Enabling NDP globally and for specific ports.....	169
Configuring NDP parameters	170
Enabling NTDP globally and for specific ports.....	170
Configuring NTDP parameters.....	171
Manually collecting topology information	171
Enabling the cluster function	172
Establishing a cluster.....	172
Enabling management VLAN autonegotiation.....	173
Configuring communication between the management switch and the member switches within a cluster	173
Configuring cluster management protocol packets	174
Cluster member management	175
Configuring the member switches	175
Enabling NDP	175
Enabling NTDP	176
Manually collecting topology information	176
Enabling the cluster function	176
Deleting a member switch from a cluster.....	176
Toggling between the CLIs of the management switch and a member switch.....	176
Adding a candidate switch to a cluster.....	177
Configuring advanced cluster management functions	177
Configuring topology management	177
Configuring interaction for a cluster.....	178

Configuring the SNMP configuration synchronization function	179
Configuring Web user accounts in batches	180
Displaying and maintaining cluster management	180
Cluster management configuration example	181
Network requirements	181
Configuration procedure	181
Configuring a stack	185
Hardware compatibility and other restrictions	185
Stack configuration task list	185
Configuring the stack master device	185
Configuring a private IP address pool for the stack	186
Configuring stack ports	186
Creating a stack	186
Configuring stack ports on a member device	186
Logging in to the CLI of a member from the master	187
Displaying and maintaining stack configuration	187
Stack configuration example	187
Support and other resources	190
Contacting HP	190
Subscription service	190
Related information	190
Documents	190
Websites	190
Conventions	191
Index	193

Using ping, tracer, and system debugging

Use the ping, tracer, and system debugging utilities to test network connectivity and identify network problems.

Ping

The ping utility sends ICMP echo requests (ECHO-REQUEST) to the destination device. Upon receiving the requests, the destination device responds with ICMP echo replies (ECHO-REPLY) to the source device. The source device outputs statistics about the ping operation, including the number of packets sent, number of echo replies received, and the round-trip time. You can measure the network performance by analyzing these statistics.

Using a ping command to test network connectivity

Task	Command	Remarks
Check whether a specified address in an IP network is reachable.	<ul style="list-style-type: none">For an IPv4 network: ping [ip] [-a <i>source-ip</i> -c <i>count</i> -f -h <i>ttl</i> -i <i>interface-type interface-number</i> -m <i>interval</i> -n -p <i>pad</i> -q -r -s <i>packet-size</i> -t <i>timeout</i> -tos <i>tos</i> -v] * <i>host</i>For an IPv6 network: ping ipv6 [-a <i>source-ipv6</i> -c <i>count</i> -m <i>interval</i> -s <i>packet-size</i> -t <i>timeout</i> -tos <i>tos</i>] * <i>host</i> [-i <i>interface-type interface-number</i>]	Use one of the commands. Available in any view.



IMPORTANT:

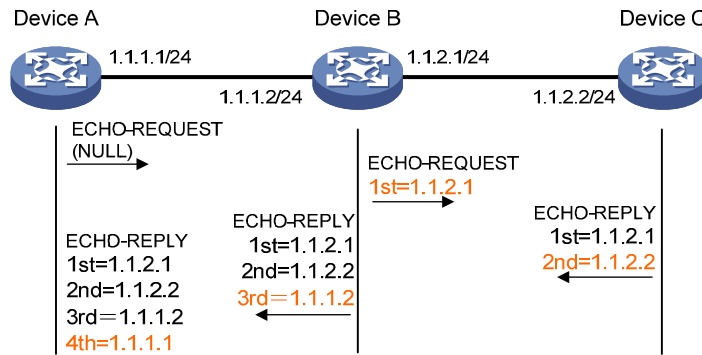
When you configure the **ping** command for a low-speed network, HP recommends that you set a larger value for the timeout timer (indicated by the **-t** keyword in the command).

Ping example

Network requirements

Test the network connectivity between Device A and Device C in [Figure 1](#). If they can reach each other, get detailed information about routes from Device A to Device C.

Figure 1 Network diagram



Test procedure

Use the **ping** command on Device A to test connectivity to Device C.

```

<DeviceA> ping 1.1.2.2
PING 1.1.2.2: 56 data bytes, press CTRL_C to break
  Reply from 1.1.2.2: bytes=56 Sequence=1 ttl=254 time=205 ms
  Reply from 1.1.2.2: bytes=56 Sequence=2 ttl=254 time=1 ms
  Reply from 1.1.2.2: bytes=56 Sequence=3 ttl=254 time=1 ms
  Reply from 1.1.2.2: bytes=56 Sequence=4 ttl=254 time=1 ms
  Reply from 1.1.2.2: bytes=56 Sequence=5 ttl=254 time=1 ms

--- 1.1.2.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
round-trip min/avg/max = 1/41/205 ms
  
```

Get detailed information about routes from Device A to Device C.

```

<DeviceA> ping -r 1.1.2.2
PING 1.1.2.2: 56 data bytes, press CTRL_C to break
  Reply from 1.1.2.2: bytes=56 Sequence=1 ttl=254 time=53 ms
    Record Route:
      1.1.2.1
      1.1.2.2
      1.1.1.2
      1.1.1.1
  Reply from 1.1.2.2: bytes=56 Sequence=2 ttl=254 time=1 ms
    Record Route:
      1.1.2.1
      1.1.2.2
      1.1.1.2
      1.1.1.1
  Reply from 1.1.2.2: bytes=56 Sequence=3 ttl=254 time=1 ms
    Record Route:
      1.1.2.1
      1.1.2.2
      1.1.1.2
  
```

```

1.1.1.1
Reply from 1.1.2.2: bytes=56 Sequence=4 ttl=254 time=1 ms
Record Route:
1.1.2.1
1.1.2.2
1.1.1.2
1.1.1.1
Reply from 1.1.2.2: bytes=56 Sequence=5 ttl=254 time=1 ms
Record Route:
1.1.2.1
1.1.2.2
1.1.1.2
1.1.1.1
--- 1.1.2.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/11/53 ms

```

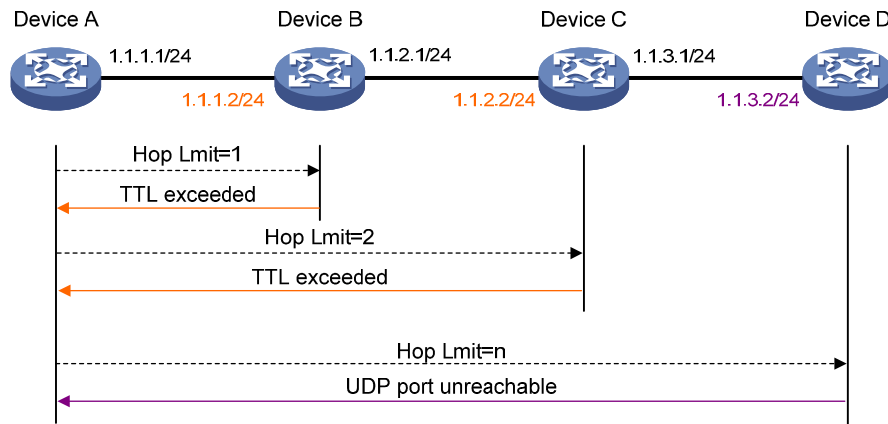
The test procedure with the **ping -r** command (see [Figure 1](#)) is as follows:

1. The source (Device A) sends an ICMP echo request with the RR option being empty to the destination (Device C).
2. The intermediate device (Device B) adds the IP address of its outbound interface (1.1.2.1) to the RR option of the ICMP echo request, and forwards the packet.
3. Upon receiving the request, the destination device copies the RR option in the request and adds the IP address of its outbound interface (1.1.2.2) to the RR option. Then the destination device sends an ICMP echo reply.
4. The intermediate device adds the IP address of its outbound interface (1.1.1.2) to the RR option in the ICMP echo reply, and then forwards the reply.
5. Upon receiving the reply, the source device adds the IP address of its inbound interface (1.1.1.1) to the RR option. Finally, you can get detailed information about routes from Device A to Device C: 1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2.

Tracert

Tracert (also called "Traceroute") enables you to get the IP addresses of Layer 3 devices in the path to a specific destination. You can use tracert to test network connectivity and identify failed nodes.

Figure 2 Network diagram



Tracert uses received ICMP error messages to get the IP addresses of devices. As shown in [Figure 2](#), tracert works as follows:

1. The source device (Device A) sends a UDP packet with a TTL value of 1 to the destination device (Device D). The destination UDP port is not used by any application on the destination device.
2. The first hop (Device B, the first Layer 3 device that receives the packet) responds by sending a TTL-expired ICMP error message to the source, with its IP address encapsulated. In this way, the source device can get the address of the first Layer 3 device (1.1.1.2).
3. The source device sends a packet with a TTL value of 2 to the destination device.
4. The second hop (Device C) responds with a TTL-expired ICMP error message, which gives the source device the address of the second Layer 3 device (1.1.2.2).
5. The process continues until the packet sent by the source device reaches the ultimate destination device. Because no application uses the destination port specified in the packet, so the destination device responds with a port-unreachable ICMP message to the source device, with its IP address 1.1.3.2 encapsulated. This way, the source device gets the IP address of the destination device (1.1.3.2).
6. The source device thinks that the packet has reached the destination device after receiving the port-unreachable ICMP message, and the path to the destination device is 1.1.1.2 to 1.1.2.2 to 1.1.3.2.

Prerequisites

Before you use a tracert command, perform the tasks in this section.

For an IPv4 network:

- Enable sending of ICMP timeout packets on the intermediate devices (the devices between the source and destination devices). If the intermediate devices are HP devices, execute the **ip ttl-expires enable** command on the devices. For more information about this command, see *Layer 3—IP Services Command Reference*.
- Enable sending of ICMP destination unreachable packets on the destination device. If the destination device is an HP device, execute the **ip unreachable enable** command. For more information about this command, see *Layer 3—IP Services Command Reference*.

For an IPv6 network:

- Enable sending of ICMPv6 timeout packets on the intermediate devices (the devices between the source and destination devices). If the intermediate devices are HP devices, execute the **ipv6**

hoplimit-expires enable command on the devices. For more information about this command, see *Layer 3—IP Services Command Reference*.

- Enable sending of ICMPv6 destination unreachable packets on the destination device. If the destination device is an HP device, execute the **ipv6 unreachable enable** command. For more information about this command, see *Layer 3—IP Services Command Reference*.

Using a tracer command to identify failed or all nodes in a path

Task	Command	Remarks
Display the routes from source to destination.	<ul style="list-style-type: none">• For an IPv4 network: tracer [-a <i>source-ip</i> -f <i>first-ttl</i> -m <i>max-ttl</i> -p <i>port</i> -q <i>packet-number</i> -tos <i>tos</i> -w <i>timeout</i>] * <i>host</i>• For an IPv6 network: tracer ipv6 [-f <i>first-ttl</i> -m <i>max-ttl</i> -p <i>port</i> -q <i>packet-number</i> -tos <i>tos</i> -w <i>timeout</i>] * <i>host</i>	<p>Use one of the commands.</p> <p>Available in any view.</p>

System debugging

The device supports various debugging for the majority of protocols and features and provides debugging information to help users diagnose errors.

Debugging information control switches

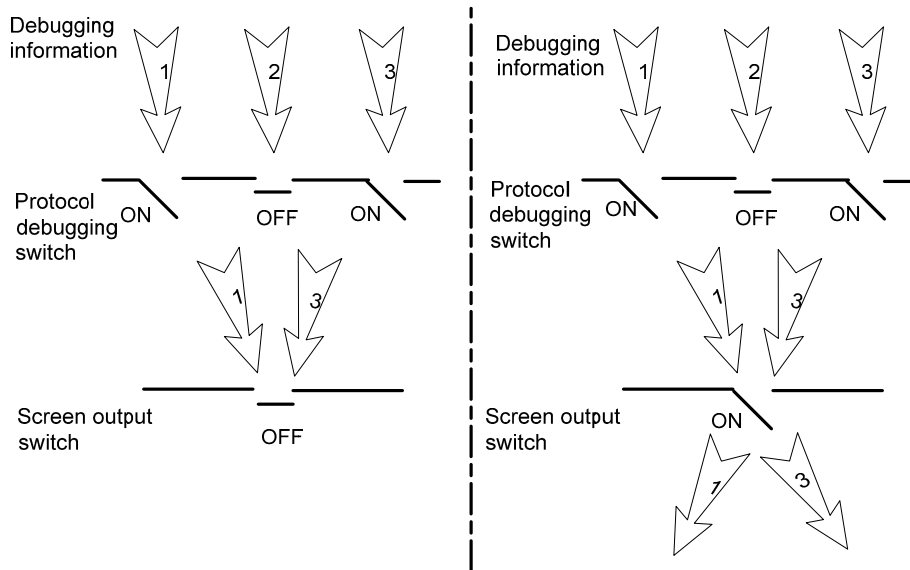
The following two switches control the display of debugging information:

- **Protocol debugging switch**—Controls protocol-specific debugging information.
- **Screen output switch**—Controls whether to display the debugging information on a certain screen.

As shown in [Figure 3](#), assume that the device can provide debugging for the three modules 1, 2, and 3. The debugging information can be output on a terminal only when both the protocol debugging switch and the screen output switch are turned on.

Output of debugging information depends on the configurations of the information center and the debugging commands of each protocol and functional module. Debugging information is typically displayed on a terminal (including console or VTY) for display. You can also send debugging information to other destinations. For more information, see "[Configuring the information center](#)."

Figure 3 Relationship between the protocol and screen output switch



Debugging a feature module

Output of debugging commands is memory intensive. To guarantee system performance, enable debugging only for modules that are in an exceptional condition. When debugging is complete, use the **undo debugging all** command to disable all the debugging functions.

Configure the **debugging**, **terminal debugging**, and **terminal monitor** commands before you can display detailed debugging information on the terminal. For more information about the **terminal debugging** and **terminal monitor** commands, see *Network Management and Monitoring Command Reference*.

To debug a feature module and display the debugging information on a terminal:

Step	Command	Remarks
1. Enable the terminal monitoring of system information.	terminal monitor	Optional. The terminal monitoring on the console is enabled by default and the terminal monitoring on the monitoring terminal is disabled by default. Available in user view.
2. Enable the terminal display of debugging information.	terminal debugging	Disabled by default. Available in user view.
3. Enable debugging for a specified module.	debugging <i>module-name</i> [<i>option</i>]	Disabled by default. Available in user view.
4. Display the enabled debugging functions.	display debugging [interface <i>interface-type interface-number</i>] [<i>module-name</i>] [{ begin exclude include } <i>regular-expression</i>]	Optional. Available in any view.

Ping and traceroute example

Network requirements

As shown in Figure 4, Device A failed to Telnet Device C. Determine whether Device A and Device C can reach each other. If they cannot reach each other, locate the failed nodes in the network.

Figure 4 Network diagram



Test procedure

1. Use the **ping** command to test connectivity between Device A and Device C.

```
<DeviceA> ping 1.1.2.2
PING 1.1.2.2: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- 1.1.2.2 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss
```

The output shows that Device A and Device C cannot reach each other.

2. Use the **tracert** command to identify failed nodes:

Enable sending of ICMP timeout packets on Device B.

```
<DeviceB> system-view
[DeviceB] ip ttl-expires enable
```

Enable sending of ICMP destination unreachable packets on Device C.

```
<DeviceC> system-view
[DeviceC] ip unreachable enable
```

Execute the **tracert** command on Device A.

```
<DeviceA> tracert 1.1.2.2
traceroute to 1.1.2.2(1.1.2.2) 30 hops max, 40 bytes packet, press CTRL_C to break
 1  1.1.1.2 14 ms 10 ms 20 ms
 2  * * *
 3  * * *
 4  * * *
 5
<DeviceA>
```

The output shows that Device A and Device C cannot reach each other, Device A and Device B can reach each other, and an error has occurred on the connection between Device B and Device C.

3. Use the **debugging ip icmp** command on Device A and Device C to verify that they can send and receive the specific ICMP packets, or use the **display ip routing-table** command to verify the availability of active routes between Device A and Device C.

Configuring NTP

Overview

NTP is typically used in large networks to dynamically synchronize time among network devices. It guarantees higher clock accuracy than manual system clock setting. In a small network that does not require high clock accuracy, you can keep time synchronized among devices by changing their system clocks one by one.

NTP runs over UDP and uses UDP port 123.

NTP application

An administrator is unable to keep time synchronized among all devices within a network by changing the system clock on each station, because this is a huge work and does not guarantee clock precision. NTP, however, allows quick clock synchronization within the entire network and ensures high clock precision.

NTP is used when all devices within the network must keep consistent time. For example:

- In analyzing log and debugging information collected from different devices in network management, time must be used as a reference basis.
- All devices must use the same reference clock in a charging system.
- To implement certain functions, such as a scheduled restart of all devices within the network, all devices must keep consistent time.
- If multiple systems process a complex event in cooperation, these systems must use the same reference clock to ensure the correct execution sequence.
- For incremental backup between a backup server and clients, timekeeping must be synchronized between the backup server and all clients.

NTP advantages

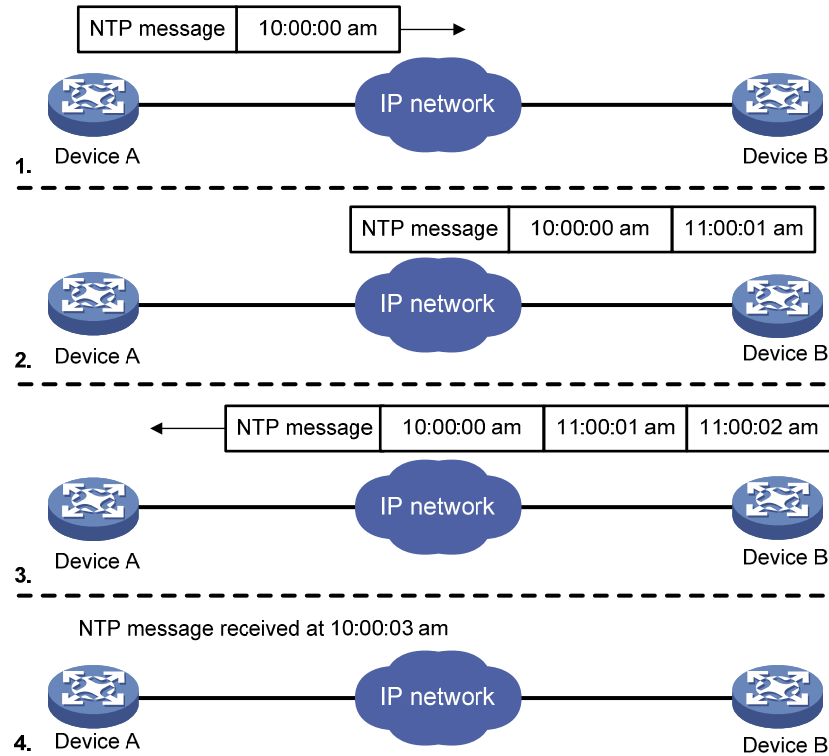
- NTP uses a stratum to describe clock accuracy. The stratum ranges from 1 to 16. Clock accuracy decreases as the stratum number increases. The stratum of a reference clock ranges from 1 to 15. A stratum 16 clock is in unsynchronized state.
- The local clock of this Switch Series cannot operate as a reference clock. It can serve as an NTP server only after it is synchronized.
- NTP supports access control and MD5 authentication.
- NTP can unicast, multicast, or broadcast protocol messages.

How NTP works

Figure 5 shows the basic workflow of NTP. Device A and Device B are connected over a network. They have their own independent system clocks, which need to be automatically synchronized through NTP. Assume that:

- Prior to system clock synchronization between Device A and Device B, the clock of Device A is set to 10:00:00 am while that of Device B is set to 11:00:00 am.
- Device B is used as the NTP time server, so Device A synchronizes to Device B.
- It takes 1 second for an NTP message to travel from one device to the other.

Figure 5 Basic workflow of NTP



The synchronization process is as follows:

- Device A sends Device B an NTP message, which is timestamped when it leaves Device A. The timestamp is 10:00:00 am (T1).
- When this NTP message arrives at Device B, it is timestamped by Device B. The timestamp is 11:00:01 am (T2).
- When the NTP message leaves Device B, Device B timestamps it. The timestamp is 11:00:02 am (T3).
- When Device A receives the NTP message, the local time of Device A is 10:00:03 am (T4).

Up to now, Device A can calculate the following parameters based on the timestamps:

- The roundtrip delay of NTP message: $\text{Delay} = (T4 - T1) - (T3 - T2) = 2 \text{ seconds}$.
- Time difference between Device A and Device B: $\text{Offset} = ((T2 - T1) + (T3 - T4)) / 2 = 1 \text{ hour}$.

Based on these parameters, Device A can synchronize its own clock to the clock of Device B.

This is a rough description of how NTP works. For more information, see RFC 1305.

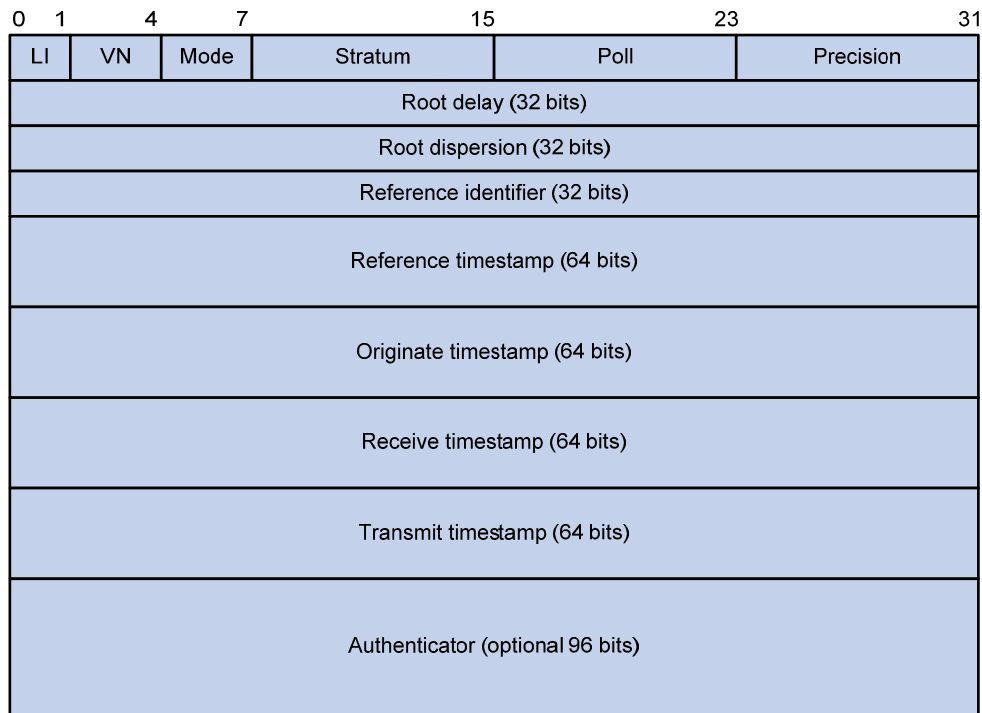
NTP message format

NTP uses two types of messages: clock synchronization and NTP control messages. All NTP messages mentioned in this document refer to NTP clock synchronization messages. NTP control messages are

used in environments where network management is needed. Because NTP control messages are not essential for clock synchronization, they are not described in this document.

A clock synchronization message is encapsulated in a UDP message in the format shown in [Figure 6](#).

Figure 6 Clock synchronization message format



The main fields are described as follows:

- **LI (Leap Indicator)**—A 2-bit leap indicator. If set to 11, it warns of an alarm condition (clock unsynchronized). If set to any other value, it is not to be processed by NTP.
- **VN (Version Number)**—A 3-bit version number that indicates the version of NTP. The latest version is version 4.
- **Mode**—A 3-bit code that indicates the operation mode of NTP. This field can be set to these values:
 - **0**—Reserved.
 - **1**—Symmetric active.
 - **2**—Symmetric passive.
 - **3**—Client.
 - **4**—Server.
 - **5**—Broadcast or multicast.
 - **6**—NTP control message.
 - **7**—Reserved for private use.
- **Stratum**—An 8-bit integer that indicates the stratum level of the local clock, with the value ranging from 1 to 16. Clock precision decreases from stratum 1 through stratum 16. A stratum 1 clock has the highest precision, and a stratum 16 clock is not synchronized.
- **Poll**—An 8-bit signed integer that indicates the maximum interval between successive messages, which is called the poll interval.
- **Precision**—An 8-bit signed integer that indicates the precision of the local clock.

- **Root Delay**—Roundtrip delay to the primary reference source.
- **Root Dispersion**—The maximum error of the local clock relative to the primary reference source.
- **Reference Identifier**—Identifier of the particular reference source.
- **Reference Timestamp**—The local time at which the local clock was last set or corrected.
- **Originate Timestamp**—The local time at which the request departed from the client for the service host.
- **Receive Timestamp**—The local time at which the request arrived at the service host.
- **Transmit Timestamp**—The local time at which the reply departed from the service host for the client.
- **Authenticator**—Authentication information.

Operation modes

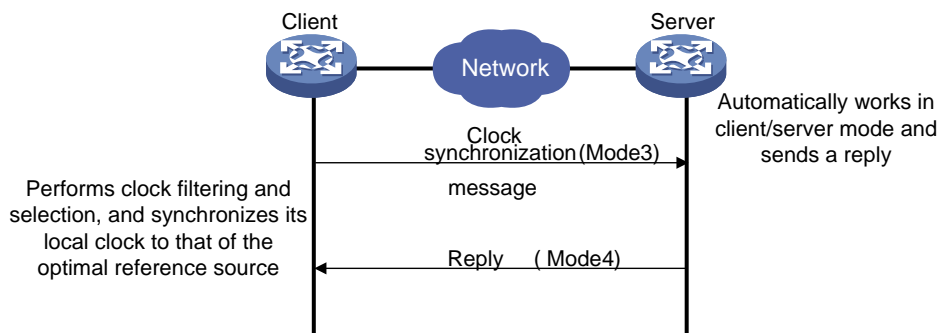
Devices that run NTP can implement clock synchronization in one of the following modes:

- Client/server mode
- Symmetric peers mode
- Broadcast mode
- Multicast mode

You can select operation modes of NTP as needed. If the IP address of the NTP server or peer is unknown and many devices in the network need to be synchronized, adopt the broadcast or multicast mode. In the client/server or symmetric peers mode, a device is synchronized from the specified server or peer, so clock reliability is enhanced.

Client/server mode

Figure 7 Client/server mode

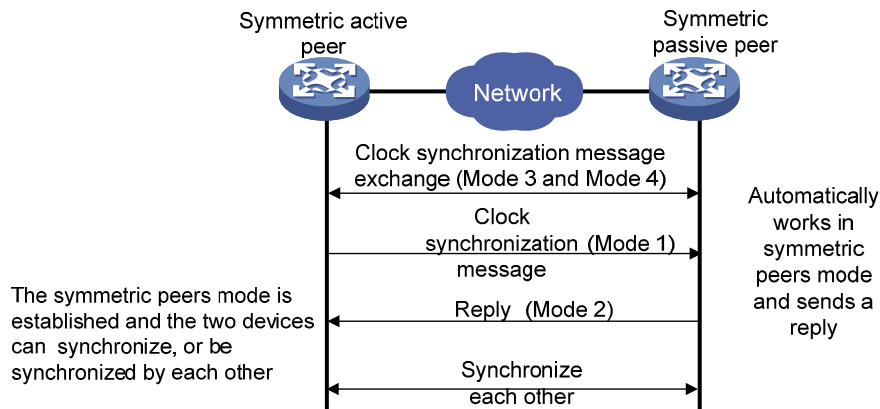


When operating in client/server mode, a client sends a clock synchronization message to servers with the Mode field in the message set to 3 (client mode). Upon receiving the message, the servers automatically operate in server mode and send a reply, with the Mode field in the messages set to 4 (server mode). Upon receiving the replies from the servers, the client performs clock filtering and selection and synchronizes to the optimal reference source.

In client/server mode, a client can synchronize to a server, but a server cannot synchronize to a client.

Symmetric peers mode

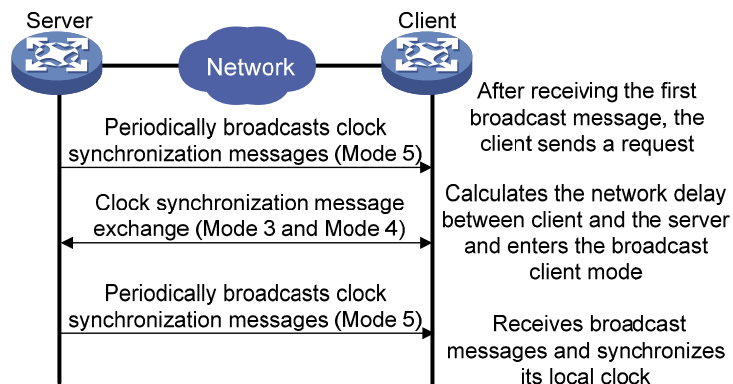
Figure 8 Symmetric peers mode



In symmetric peers mode, devices that operate in symmetric active mode and symmetric passive mode exchange NTP messages with the Mode field 3 (client mode) and 4 (server mode). Then the device that operates in symmetric active mode periodically sends clock synchronization messages, with the Mode field in the messages set to 1 (symmetric active). The device that receives the messages automatically enters symmetric passive mode and sends a reply, with the Mode field in the message set to 2 (symmetric passive). This exchange of messages establishes symmetric peers mode between the two devices, so the two devices can synchronize, or be synchronized by, each other. If the clocks of both devices have been synchronized, the device whose local clock has a lower stratum level synchronizes the other device.

Broadcast mode

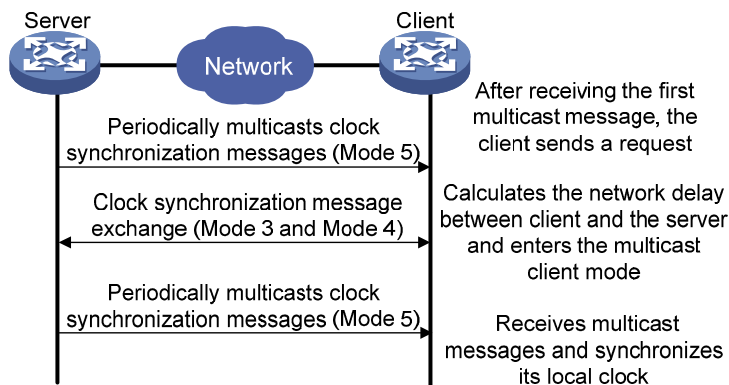
Figure 9 Broadcast mode



In broadcast mode, a server periodically sends clock synchronization messages to broadcast address 255.255.255.255, with the Mode field in the messages set to 5 (broadcast mode). Clients listen to the broadcast messages from servers. When a client receives the first broadcast message, the client and the server start to exchange messages with the Mode field set to 3 (client mode) and 4 (server mode), to calculate the network delay between client and the server. Then, the client enters broadcast client mode. The client continues listening to broadcast messages, and synchronizes its local clock based on the received broadcast messages.

Multicast mode

Figure 10 Multicast mode



In multicast mode, a server periodically sends clock synchronization messages to the user-configured multicast address, or, if no multicast address is configured, to the default NTP multicast address 224.0.1.1, with the Mode field in the messages set to 5 (multicast mode). Clients listen to the multicast messages from servers. When a client receives the first multicast message, the client and the server start to exchange messages with the Mode field set to 3 (client mode) and 4 (server mode), to calculate the network delay between client and server. Then, the client enters multicast client mode. It continues listening to multicast messages, and synchronizes its local clock based on the received multicast messages.

In symmetric peers mode, broadcast mode, and multicast mode, the client (or the symmetric active peer) and the server (the symmetric passive peer) can operate in the specified NTP operation mode only after they exchange NTP messages with the Mode field 3 (client mode) and the Mode field 4 (server mode). During this message exchange process, NTP clock synchronization can be implemented.

NTP configuration task list

Task	Remarks
Configuring NTP operation modes	Required.
Configuring optional parameters	Optional.
Configuring access-control rights	Optional.
Configuring NTP authentication	Optional.

Configuring NTP operation modes

Devices can implement clock synchronization in one of the following modes:

- **Client/server mode**—Configure only clients.
- **Symmetric mode**—Configure only symmetric-active peers.
- **Broadcast mode**—Configure both clients and servers.
- **Multicast mode**—Configure both clients and servers.

Configuring the client/server mode

For devices operating in client/server mode, make configurations on the clients.

If you specify the source interface for NTP messages by specifying the source interface source-interface option, NTP uses the primary IP address of the specified interface as the source IP address of the NTP messages.

A device can act as a server to synchronize other devices only after it is synchronized. If a server has a stratum level higher than or equal to a client, the client will not synchronize to that server.

To specify an NTP server on the client:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify an NTP server for the device.	ntp-service unicast-server { <i>ip-address</i> <i>server-name</i> } [authentication-keyid <i>keyid</i> priority source-interface <i>interface-type interface-number</i> version <i>number</i>] *	By default, no NTP server is specified. In this command, the <i>ip-address</i> argument must be a unicast address, rather than a broadcast address, a multicast address or the IP address of the local clock. You can configure multiple servers by repeating the command. The clients will select the optimal reference source.

Configuring the symmetric peers mode

Follow these guidelines when you configure the NTP symmetric peers mode:

- For devices operating in symmetric mode, specify a symmetric-passive peer on a symmetric-active peer.
- Use any NTP configuration command in [Configuring NTP operation modes](#) to enable NTP. Otherwise, a symmetric-passive peer does not process NTP messages from a symmetric-active peer.
- Either the symmetric-active peer or the symmetric-passive peer must be in synchronized state. Otherwise, clock synchronization does not proceed.

To specify a symmetric-passive peer on the active peer:

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

Step	Command	Remarks
2. Specify a symmetric-passive peer for the device.	<pre>ntp-service unicast-peer { ip-address peer-name } [authentication-keyid keyid priority source-interface interface-type interface-number version number] *</pre>	<p>By default, no symmetric-passive peer is specified.</p> <p>The <i>ip-address</i> argument must be a unicast address, rather than a broadcast address, a multicast address, or the IP address of the local clock.</p> <p>After you specify the source interface for NTP messages by specifying the source interface <i>source-interface</i> option, the source IP address of the NTP messages is set as the primary IP address of the specified interface.</p> <p>You can configure multiple symmetric-passive peers by repeating this command.</p>

Configuring the broadcast mode

The broadcast server periodically sends NTP broadcast messages to the broadcast address 255.255.255.255. After receiving the messages, the device operating in NTP broadcast client mode sends a reply and synchronizes to the server.

Configure the NTP broadcast mode on both the server and clients. The NTP broadcast mode can only be configured in a specific interface view because an interface needs to be specified on the broadcast server for sending NTP broadcast messages and on each broadcast client for receiving broadcast messages.

Configuring a broadcast client

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	This command enters the view of the interface for sending NTP broadcast messages.
3. Configure the device to operate in NTP broadcast client mode.	ntp-service broadcast-client	N/A

Configuring the broadcast server

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	This command enters the view of the interface for sending NTP broadcast messages.

Step	Command	Remarks
3. Configure the device to operate in NTP broadcast server mode.	ntp-service broadcast-server [authentication-keyid <i>keyid</i> version <i>number</i>] *	A broadcast server can synchronize broadcast clients only when its clock has been synchronized.

Configuring the multicast mode

The multicast server periodically sends NTP multicast messages to multicast clients, which send replies after receiving the messages and synchronize their local clocks.

Configure the NTP multicast mode on both the server and clients. The NTP multicast mode must be configured in a specific interface view.

Configuring a multicast client

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	This command enters the view of the interface for sending NTP multicast messages.
3. Configure the device to operate in NTP multicast client mode.	ntp-service multicast-client [<i>ip-address</i>]	You can configure up to 1024 multicast clients, of which 128 can take effect at the same time.

Configuring the multicast server

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	This command enters the view of the interface for sending NTP multicast messages.
3. Configure the device to operate in NTP multicast server mode.	ntp-service multicast-server [<i>ip-address</i>] [authentication-keyid <i>keyid</i> ttl <i>ttl-number</i> version <i>number</i>] *	A multicast server can synchronize broadcast clients only when its clock has been synchronized.

Configuring optional parameters

This section explains how to configure the optional parameters of NTP.

Specifying the source interface for NTP messages

If you specify the source interface for NTP messages, the device sets the source IP address of the NTP messages as the primary IP address of the specified interface when sending the NTP messages. NTP packets might not be received due to state changes of an interface on the device. To avoid that problem, specify the loopback interface as the source interface.

When the device responds to an NTP request received, the source IP address of the NTP response is always the destination IP address of the NTP request.

Configuration guidelines

- The source interface for NTP unicast messages is the interface specified in the **ntp-service unicast-server** or **ntp-service unicast-peer** command.
- The source interface for NTP broadcast or multicast messages is the interface where you configure the **ntp-service broadcast-server** or **ntp-service multicast-server** command.

Configuration procedure

To specify the source interface for NTP messages:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify the source interface for NTP messages.	ntp-service source-interface <i>interface-type interface-number</i>	By default, no source interface is specified for NTP messages, and the system uses the IP address of the interface determined by the matching route as the source IP address of NTP messages.

Disabling an interface from receiving NTP messages

If NTP is enabled, NTP messages can be received from all interfaces by default. You can disable an interface from receiving NTP messages by using the following configuration.

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Disable the interface from receiving NTP messages.	ntp-service in-interface disable	By default, an interface is enabled to receive NTP messages.

Configuring the allowed maximum number of dynamic sessions

NTP has the following types of associations:

- **Static association**—An association that a user has manually created by using an NTP command.
- **Dynamic association**—Temporary association created by the system during operation. A dynamic association is removed if the system fails to receive messages from it over a specific period of time.

The following describes how an association is established in different operation modes:

- **Client/server mode**—After you specify an NTP server, the system creates a static association on the client. The server simply responds passively upon the receipt of a message, rather than creating an association (static or dynamic).

- **Symmetric active/passive mode**—After you specify a symmetric-passive peer on a symmetric active peer, static associations are created on the symmetric-active peer, and dynamic associations are created on the symmetric-passive peer.
- **Broadcast or multicast mode**—Static associations are created on the server, and dynamic associations are created on the client.

A single device can have a maximum of 128 concurrent associations, including static associations and dynamic associations.

To configure the allowed maximum number of dynamic sessions:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the maximum number of dynamic sessions allowed to be established locally.	ntp-service max-dynamic-sessions number	The default is 100.

Configuring the DSCP value for NTP messages

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the Differentiated Service Code Point (DSCP) value for NTP messages.	ntp-service dscp dscp-value	The default setting is 16.

Configuring access-control rights

From the highest to lowest, the NTP service access-control rights are **peer**, **server**, **synchronization**, and **query**. If a device receives an NTP request, it performs an access-control right match and uses the first matched right. If no matched right is found, the device drops the NTP request.

- **Query**—Control query permitted. This level of right permits the peer devices to perform control query to the NTP service on the local device, but it does not permit a peer device to synchronize to the local device. "Control query" refers to the query of some states of the NTP service, including alarm information, authentication status, and clock source information.
- **Synchronization**—Server access only. This level of right permits a peer device to synchronize to the local device, but it does not permit the peer devices to perform control query.
- **Server**—Server access and query permitted. This level of right permits the peer devices to perform synchronization and control query to the local device, but it does not permit the local device to synchronize to a peer device.
- **Peer**—Full access. This level of right permits the peer devices to perform synchronization and control query to the local device, and it permits the local device to synchronize to a peer device.

The access-control right mechanism provides only a minimum level of security protection for a system running NTP. A more secure method is identity authentication.

Configuration prerequisites

Before you configure the NTP service access-control right to the local device, create and configure an ACL associated with the access-control right. For more information about ACLs, see *ACL and QoS Configuration Guide*.

Configuration procedure

To configure the NTP service access-control right to the local device:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the NTP service access-control right for a peer device to access the local device.	ntp-service access { peer query server synchronization } acl-number	The default is peer .

Configuring NTP authentication

Enable NTP authentication for a system running NTP in a network where there is a high security demand. NTP authentication enhances network security by using client-server key authentication, which prohibits a client from synchronizing with a device that fails authentication.

To configure NTP authentication, do the following:

- Enable NTP authentication
- Configure an authentication key
- Configure the key as a trusted key
- Associate the specified key with an NTP server or a symmetric peer

These tasks are required. If any task is omitted, NTP authentication cannot function.

Configuring NTP authentication in client/server mode

Follow these instructions to configure NTP authentication in client/server mode:

- A client can synchronize to the server only when you configure all the required tasks on both the client and server.
- On the client, if NTP authentication is not enabled or no key is specified to associate with the NTP server, the client is not authenticated. No matter whether NTP authentication is enabled or not on the server, the clock synchronization between the server and client can be performed.
- On the client, if NTP authentication is enabled and a key is specified to associate with the NTP server, but the key is not a trusted key, the client does not synchronize to the server no matter whether NTP authentication is enabled or not on the server.

Configuring NTP authentication for client

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

Step	Command	Remarks
2. Enable NTP authentication.	ntp-service authentication enable	By default, NTP authentication is disabled.
3. Configure an NTP authentication key.	ntp-service authentication-keyid <i>keyid</i> authentication-mode md5 [cipher simple] <i>value</i>	By default, no NTP authentication key is configured. Configure the same authentication key on the client and server.
4. Configure the key as a trusted key.	ntp-service reliable authentication-keyid <i>keyid</i>	By default, the authentication key is not configured as a trusted key.
5. Associate the specified key with an NTP server.	<ul style="list-style-type: none"> Client/server mode: ntp-service unicast-server { <i>ip-address</i> <i>server-name</i> } authentication-keyid <i>keyid</i> Symmetric peers mode: ntp-service unicast-peer { <i>ip-address</i> <i>peer-name</i> } authentication-keyid <i>keyid</i> 	You can associate a non-existing key with an NTP server. To make NTP authentication effective, you must configure the key as an authentication key and specify it as a trusted key after associating the key with the NTP server.

Configuring NTP authentication for a server

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable NTP authentication.	ntp-service authentication enable	By default, NTP authentication is disabled.
3. Configure an NTP authentication key.	ntp-service authentication-keyid <i>keyid</i> authentication-mode md5 [cipher simple] <i>value</i>	By default, no NTP authentication key is configured. Configure the same authentication key on the client and server.
4. Configure the key as a trusted key.	ntp-service reliable authentication-keyid <i>keyid</i>	By default, the authentication key is not configured as a trusted key.
5. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
6. Associate the specified key with an NTP server.	<ul style="list-style-type: none"> Broadcast server mode: ntp-service broadcast-server authentication-keyid <i>keyid</i> Multicast server mode: ntp-service multicast-server authentication-keyid <i>keyid</i> 	You can associate a non-existing key with an NTP server. To enable NTP authentication, you must configure the key and specify it as a trusted key after associating the key with the NTP server.

Displaying and maintaining NTP

Task	Command	Remarks
Display information about NTP service status.	display ntp-service status [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

Task	Command	Remarks
Display information about NTP sessions.	display ntp-service sessions [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display brief information about the NTP servers from the local device back to the primary reference source.	display ntp-service trace [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

NTP configuration examples

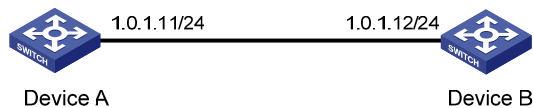
This section provides configuration examples for NTP.

Configuring the client/server mode

Network requirements

As shown in [Figure 11](#), configure Device A as a reference source, with the stratum level 2. Configure Device B to operate in client/server mode and use Device A as its NTP server.

Figure 11 Network diagram



Configuration procedure

- Set the IP address for each interface as shown in [Figure 11](#). (Details not shown.)
- Configure Device B:


```

# Display the NTP status of Device B before clock synchronization.
<DeviceB> display ntp-service status
Clock status: unsynchronized
Clock stratum: 16
Reference clock ID: none
Nominal frequency: 64.0000 Hz
Actual frequency: 64.0000 Hz
Clock precision: 2^7
Clock offset: 0.0000 ms
Root delay: 0.00 ms
Root dispersion: 0.00 ms
Peer dispersion: 0.00 ms
Reference time: 00:00:00.000 UTC Jan 1 1900 (00000000.00000000)

# Specify Device A as the NTP server of Device B so Device B synchronizes to Device A.
<DeviceB> system-view
[DeviceB] ntp-service unicast-server 1.0.1.11

# Display the NTP status of Device B after clock synchronization.
[DeviceB] display ntp-service status
Clock status: synchronized
      
```

```

Clock stratum: 3
Reference clock ID: 1.0.1.11
Nominal frequency: 64.0000 Hz
Actual frequency: 64.0000 Hz
Clock precision: 2^7
Clock offset: 0.0000 ms
Root delay: 31.00 ms
Root dispersion: 1.05 ms
Peer dispersion: 7.81 ms
Reference time: 14:53:27.371 UTC Sep 19 2005 (C6D94F67.5EF9DB22)

```

The output shows that Device B has synchronized to Device A because it has a higher stratum than Device A.

Display NTP session information for Device B.

```

[DeviceB] display ntp-service sessions
          source      reference  stra reach poll now offset delay disper
*****
[12345] 1.0.1.11 127.127.1.0    2    63   64   3  -75.5   31.0  16.5
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations : 1

```

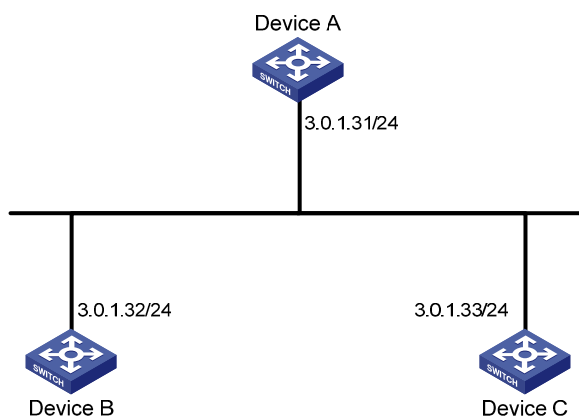
The output shows that an association has been set up between Device B and Device A.

Configuring the NTP symmetric mode

Network requirements

- As shown in Figure 12, configure Device A as a reference source, with the stratum level 2.
- Configure Device B to operate in client mode and use Device A as its NTP server.
- Configure Device C to operate in symmetric-active mode and use Device B as its symmetric-passive peer.

Figure 12 Network diagram



Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure Device B:
 - # Specify Device A as the NTP server of Device B.

```
<DeviceB> system-view
[DeviceB] ntp-service unicast-server 3.0.1.31
```

3. Display the NTP status of Device B after clock synchronization.

```
[DeviceB] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: -21.1982 ms
Root delay: 15.00 ms
Root dispersion: 775.15 ms
Peer dispersion: 34.29 ms
Reference time: 15:22:47.083 UTC Sep 19 2005 (C6D95647.153F7CED)
```

The output shows that Device B has synchronized to Device A because it has a higher stratum than Device A.

4. Configure Device C (after Device B is synchronized to Device A):

Configure Device C as a symmetric peer after local synchronization.

```
[DeviceC] ntp-service unicast-peer 3.0.1.32
```

The output shows that Device B and Device C are configured as symmetric peers, with Device C in symmetric-active mode and Device B in symmetric-passive mode. Because the stratus level of Device C is 16 while that of Device B is 3, Device B synchronizes to Device C.

Display the NTP status of Device C after clock synchronization.

```
[DeviceC] display ntp-service status
Clock status: synchronized
Clock stratum: 4
Reference clock ID: 3.0.1.32
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: -21.1982 ms
Root delay: 15.00 ms
Root dispersion: 775.15 ms
Peer dispersion: 34.29 ms
Reference time: 15:22:47.083 UTC Sep 19 2005 (C6D95647.153F7CED)
```

The output shows that Device C has synchronized to Device B because it has a higher stratum than Device B.

Display NTP session information for Device C.

```
[DeviceC] display ntp-service sessions
          source          reference      stra reach poll  now offset  delay disper
*****
[12345] 3.0.1.32          3.0.1.31          3    3    64    16    -6.4    4.8    1.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations : 1
```

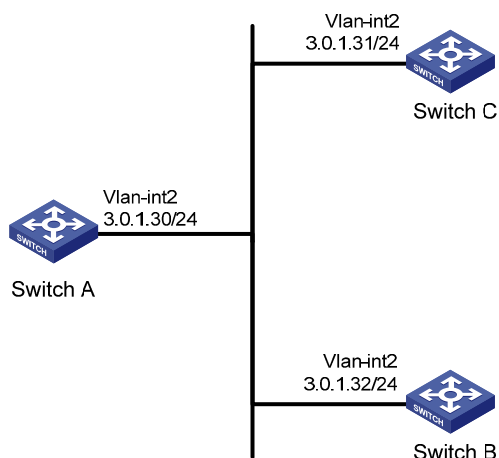
The output shows that an association has been set up between Device B and Device C.

Configuring NTP broadcast mode

Network requirements

- As shown in [Figure 13](#), configure Switch C as a reference source, with the stratum level 2.
- Configure Switch C to operate in broadcast server mode and send broadcast messages from VLAN-interface 2.
- Configure Switch A and Switch B to operate in broadcast client mode, and listen to broadcast messages through their VLAN-interface 2 respectively.

Figure 13 Network diagram



Configuration procedure

1. Set the IP address for each interface as shown in [Figure 13](#). (Details not shown.)
2. Configure Switch C:
Configure Switch C to operate in broadcast server mode and send broadcast messages through VLAN-interface 2.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service broadcast-server
```
3. Configure Switch A:
Configure Switch A to operate in broadcast client mode and receive broadcast messages on VLAN-interface 2.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ntp-service broadcast-client
```
4. Configure Switch B:
Configure Switch B to operate in broadcast client mode and receive broadcast messages on VLAN-interface 2.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ntp-service broadcast-client
```

Switch A and Switch B get synchronized upon receiving a broadcast message from Switch C.

Take Switch A as an example. Display the NTP status of Switch A after clock synchronization.

```
[SwitchA-Vlan-interface2] display ntp-service status
```

```

Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 64.0000 Hz
Actual frequency: 64.0000 Hz
Clock precision: 2^7
Clock offset: 0.0000 ms
Root delay: 31.00 ms
Root dispersion: 8.31 ms
Peer dispersion: 34.30 ms
Reference time: 16:01:51.713 UTC Sep 19 2005 (C6D95F6F.B6872B02)

```

The output shows that Switch A has synchronized to Switch C because it has a higher stratum than Switch C.

Display NTP session information for Switch A.

```

[SwitchA-Vlan-interface2] display ntp-service sessions
      source      reference      stra reach poll now offset delay disper
*****
[1234] 3.0.1.31  127.127.1.0    2   254    64   62  -16.0   32.0   16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations : 1

```

The output shows that an association has been set up between Switch A and Switch C.

Configuring NTP multicast mode

Network requirements

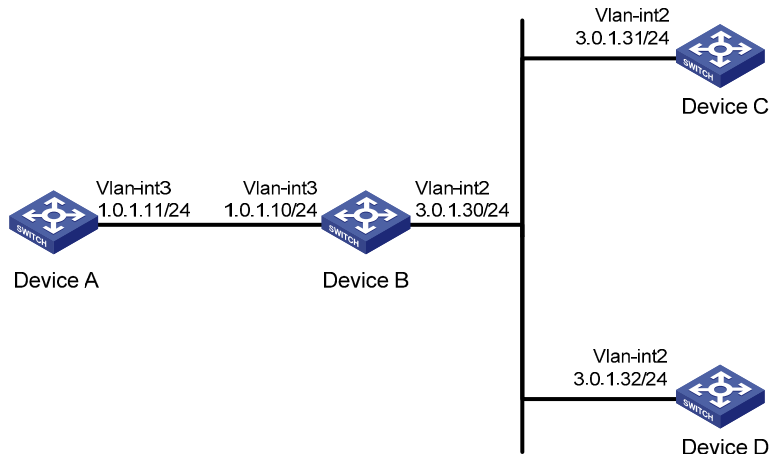
As shown in [Figure 14](#), configure Device C as a reference source, with the stratum level 2.

- Configure Device C to operate in multicast server mode and send multicast messages from VLAN-interface 2.
- Configure Device A and Device D to operate in multicast client mode and receive multicast messages through VLAN-interface 3 and VLAN-interface 2 respectively.

NOTE:

In this example, Switch B must be a Layer 3 switch that supports multicast routing.

Figure 14 Network diagram



Configuration procedure

1. Set the IP address for each interface as shown in Figure 14. (Details not shown.)
2. Configure Device C:
Configure Device C to operate in multicast server mode and send multicast messages through VLAN-interface 2.

```
[DeviceC] interface vlan-interface 2
[DeviceC-Vlan-interface2] ntp-service multicast-server
```

3. Configure Device D:
Configure Device D to operate in multicast client mode and receive multicast messages on VLAN-interface 2.

```
<DeviceD> system-view
[DeviceD] interface vlan-interface 2
[DeviceD-Vlan-interface2] ntp-service multicast-client
```

Because Device D and Device C are on the same subnet, Device D can receive the multicast messages from Device C without being enabled with the multicast functions and can synchronize to Device C.

Display the NTP status of Device D after clock synchronization.

```
[DeviceD-Vlan-interface2] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 64.0000 Hz
Actual frequency: 64.0000 Hz
Clock precision: 2^7
Clock offset: 0.0000 ms
Root delay: 31.00 ms
Root dispersion: 8.31 ms
Peer dispersion: 34.30 ms
Reference time: 16:01:51.713 UTC Sep 19 2005 (C6D95F6F.B6872B02)
```

The output shows that Device D has synchronized to Device C because it has a higher stratum than Device C.

Display NTP session information for Device D.

```
[DeviceD-Vlan-interface2] display ntp-service sessions
      source      reference      stra reach poll now offset delay disper
*****
[1234] 3.0.1.31 127.127.1.0 2 254 64 62 -16.0 31.0 16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations : 1
```

The output shows that an association has been set up between Device D and Device C.

4. Configure Device B:

Because Device A and Device C are on different subnets, you must enable the multicast functions on Device B before Device A can receive multicast messages from Device C.

Enable IP multicast routing and IGMP.

```
<DeviceB> system-view
[DeviceB] multicast routing-enable
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] pim dm
[DeviceB-Vlan-interface2] quit
[DeviceB] vlan 3
[DeviceB-vlan3] port gigabitethernet 1/0/1
[DeviceB-vlan3] quit
[DeviceB] interface vlan-interface 3
[DeviceB-Vlan-interface3] igmp enable
[DeviceB-Vlan-interface3] igmp static-group 224.0.1.1
[DeviceB-Vlan-interface3] quit
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] igmp-snooping static-group 224.0.1.1 vlan 3
```

5. Configure Device A:

```
<DeviceA> system-view
[DeviceA] interface vlan-interface 3
```

Configure Device A to operate in multicast client mode and receive multicast messages on VLAN-interface 3.

```
[DeviceA-Vlan-interface3] ntp-service multicast-client
```

Display the NTP status of Device A after clock synchronization.

```
[DeviceA-Vlan-interface3] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 64.0000 Hz
Actual frequency: 64.0000 Hz
Clock precision: 2^7
Clock offset: 0.0000 ms
Root delay: 40.00 ms
Root dispersion: 10.83 ms
Peer dispersion: 34.30 ms
Reference time: 16:02:49.713 UTC Sep 19 2005 (C6D95F6F.B6872B02)
```

The output shows that Device A has synchronized to Device C because it has a higher stratum than Device C.

```
# Display NTP session information for Device A.
```

```
[DeviceA-Vlan-interface3] display ntp-service sessions
      source      reference      stra reach poll now offset delay disper
*****
[1234] 3.0.1.31 127.127.1.0 2 255 64 26 -16.0 40.0 16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations : 1
```

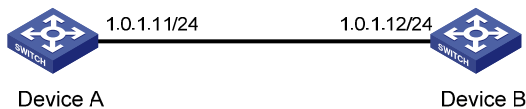
The output shows that an association has been set up between Device A and Device C.

Configuring NTP client/server mode with authentication

Network requirements

- As shown in [Figure 15](#), configure Device A as a reference source, with the stratum level 2.
- Configure Device B to operate in client mode and use Device A as its NTP server.
- Enable NTP authentication on both Device A and Device B.

Figure 15 Network diagram



Configuration procedure

1. Set the IP address for each interface as shown in [Figure 15](#). (Details not shown.)
2. Configure Device B:

```
<DeviceB> system-view
# Enable NTP authentication on Device B.
[DeviceB] ntp-service authentication enable
# Set an authentication key.
[DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
# Specify the key as a trusted key.
[DeviceB] ntp-service reliable authentication-keyid 42
# Specify Device A as the NTP server of Device B.
[DeviceB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

Before Device B can synchronize to Device A, enable NTP authentication for Device A.
3. Configure Device A:

```
# Enable NTP authentication.
[DeviceA] ntp-service authentication enable
# Set an authentication key.
[DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
# Specify the key as a trusted key.
[DeviceA] ntp-service reliable authentication-keyid 42
# Display the NTP status of Device B after clock synchronization.
[DeviceB] display ntp-service status
Clock status: synchronized
```

```

Clock stratum: 3
Reference clock ID: 1.0.1.11
Nominal frequency: 64.0000 Hz
Actual frequency: 64.0000 Hz
Clock precision: 2^7
Clock offset: 0.0000 ms
Root delay: 31.00 ms
Root dispersion: 1.05 ms
Peer dispersion: 7.81 ms
Reference time: 14:53:27.371 UTC Sep 19 2005 (C6D94F67.5EF9DB22)

```

The output shows that Device B has synchronized to Device A because it has a higher stratum than Device A.

Display NTP session information for Device B.

```

[DeviceB] display ntp-service sessions
          source      reference  stra reach poll now offset delay disper
*****
[12345] 1.0.1.11 127.127.1.0    2    63   64   3  -75.5   31.0  16.5
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations : 1

```

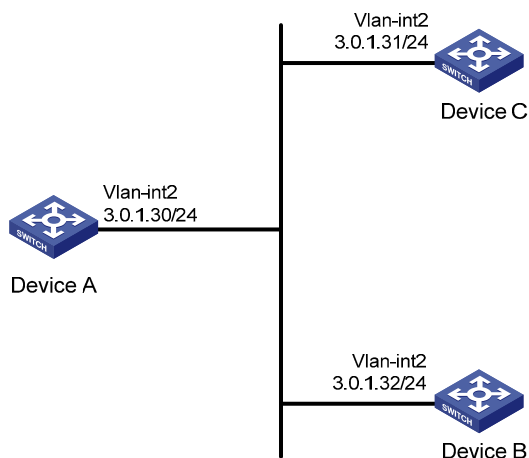
The output shows that an association has been set up Device B and Device A.

Configuring NTP broadcast mode with authentication

Network requirements

- As shown in [Figure 16](#), configure Device C as a reference source, with the stratum level 3.
- Configure Device C to operate in broadcast server mode and send broadcast messages from VLAN-interface 2.
- Configure Device A and Device B to operate in broadcast client mode and receive broadcast messages through VLAN-interface 2.
- Enable NTP authentication on both Device B and Device C.

Figure 16 Network diagram



Configuration procedure

1. Set the IP address for each interface as shown in [Figure 16](#). (Details not shown.)
2. Configure Device A:
Configure the Device A to operate in NTP broadcast client mode and receive NTP broadcast messages on VLAN-interface 2.

```
<DeviceA> system-view
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ntp-service broadcast-client
```
3. Configure Device B:
Enable NTP authentication on Device B. Configure an NTP authentication key, with the key ID 88 and key value 123456, and specify the key as a trusted key.

```
<DeviceB> system-view
[DeviceB] ntp-service authentication enable
[DeviceB] ntp-service authentication-keyid 88 authentication-mode md5 123456
[DeviceB] ntp-service reliable authentication-keyid 88
```


Configure Device B to operate in broadcast client mode and receive NTP broadcast messages on VLAN-interface 2.

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ntp-service broadcast-client
```
4. Configure Device C:
Configure Device C to operate in NTP broadcast server mode and use VLAN-interface 2 to send NTP broadcast packets.

```
[DeviceC] interface vlan-interface 2
[DeviceC-Vlan-interface2] ntp-service broadcast-server
[DeviceC-Vlan-interface2] quit
```


Display NTP service status information on Device A.

```
[DeviceA-Vlan-interface2] display ntp-service status
Clock status: synchronized
Clock stratum: 4
Reference clock ID: 3.0.1.31
Nominal frequency: 64.0000 Hz
Actual frequency: 64.0000 Hz
Clock precision: 2^7
Clock offset: 0.0000 ms
Root delay: 31.00 ms
Root dispersion: 8.31 ms
Peer dispersion: 34.30 ms
Reference time: 16:01:51.713 UTC Sep 19 2005 (C6D95F6F.B6872B02)
```

The output shows that Device A has synchronized to Device C because it has a higher stratum than Device C.

Display NTP session information for Device A.

```
[DeviceA-Vlan-interface2] display ntp-service sessions
      source      reference      stra reach poll now offset delay disper
*****
[1234] 3.0.1.31 127.127.1.0 3 254 64 62 -16.0 32.0 16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

Total associations : 1

The output shows that an association has been set up Device A and Device C.

Display NTP service status information on Device B.

```
[DeviceB-Vlan-interface2] display ntp-service status
Clock status: unsynchronized
Clock stratum: 16
Reference clock ID: none
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 0.0000 ms
Root delay: 0.00 ms
Root dispersion: 0.00 ms
Peer dispersion: 0.00 ms
Reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

The output shows that NTP authentication is enabled on Device B, but not enabled on Device C. Therefore, Device B cannot synchronize to Device C.

Enable NTP authentication Device C. Configure an NTP authentication key, with the key ID 88 and key value 123456, and specify the key as a trusted key.

```
[DeviceC] ntp-service authentication enable
[DeviceC] ntp-service authentication-keyid 88 authentication-mode md5 123456
[DeviceC] ntp-service reliable authentication-keyid 88
```

Specify Device C as an NTP broadcast server, and associate the key 88 with Device C.

```
[DeviceC] interface vlan-interface 2
[DeviceC-Vlan-interface2] ntp-service broadcast-server authentication-keyid 88
```

Display NTP service status information on Device B.

```
[DeviceB-Vlan-interface2] display ntp-service status
Clock status: synchronized
Clock stratum: 4
Reference clock ID: 3.0.1.31
Nominal frequency: 64.0000 Hz
Actual frequency: 64.0000 Hz
Clock precision: 2^7
Clock offset: 0.0000 ms
Root delay: 31.00 ms
Root dispersion: 8.31 ms
Peer dispersion: 34.30 ms
Reference time: 16:01:51.713 UTC Sep 19 2005 (C6D95F6F.B6872B02)
```

The output shows that Device B has synchronized to Device C because it has a higher stratum than Device C.

Display NTP session information for Device B.

```
[DeviceB-Vlan-interface2] display ntp-service sessions
      source      reference      stra reach poll now offset delay disper
*****
[1234] 3.0.1.31 127.127.1.0 3 254 64 62 -16.0 32.0 16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations : 1
```


The output shows that an association has been set up between Device B and Device C.

Display NTP service status information on Device A.

```
[DeviceA-Vlan-interface2] display ntp-service status
```

```
Clock status: synchronized
```

```
Clock stratum: 4
```

```
Reference clock ID: 3.0.1.31
```

```
Nominal frequency: 64.0000 Hz
```

```
Actual frequency: 64.0000 Hz
```

```
Clock precision: 2^7
```

```
Clock offset: 0.0000 ms
```

```
Root delay: 31.00 ms
```

```
Root dispersion: 8.31 ms
```

```
Peer dispersion: 34.30 ms
```

```
Reference time: 16:01:51.713 UTC Sep 19 2005 (C6D95F6F.B6872B02)
```

The output shows that configuring NTP authentication on Device C does not affect Device A and Device A still synchronizes to Device C.

Configuring the information center

This chapter describes how to configure the information center.

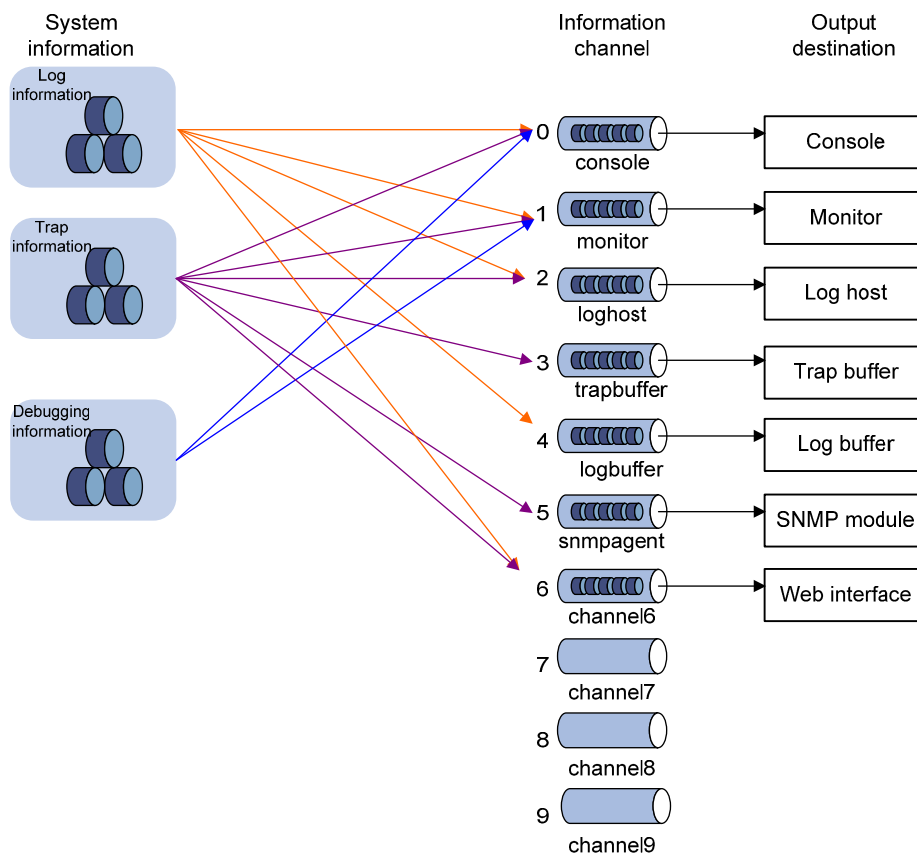
Overview

The information center collects and classifies system information as follows:

- Receives system information including log, trap, and debug information from source modules.
- Outputs the information to different information channels, according to output rules.
- Outputs information to different destinations, based on channel-to-destination associations.

Information center assigns log, trap, and debug information to 10 information channels according to eight severity levels and then outputs the information to different destinations. The following describes the working process in detail.

Figure 17 Information center diagram (default)



By default, the information center is enabled. It affects system performance to some degree when it is processing large amounts of information. If the system resources are insufficient, disable the information center to save resources.

Classification of system information

System information is divided into the following types:

- Log information
- Trap information
- Debug information

System information levels

System information is classified into eight severity levels, from 0 through 7 in descending order. The device outputs the system information with a severity level that is higher than or equal to the specified level. For example, if you configure an output rule with a severity level of 6 (informational), information that has a severity level from 0 to 6 is output.

Table 1 Severity description

Severity	Severity value	Description	Corresponding keyword in commands
Emergency	0	The system is unusable.	emergencies
Alert	1	Action must be taken immediately.	alerts
Critical	2	Critical condition.	critical
Error	3	Error condition.	errors
Warning	4	Warning condition.	warnings
Notification	5	Normal but significant condition.	notifications
Informational	6	Informational message.	informational
Debug	7	Debug message.	debugging

Output channels and destinations

Table 2 shows the output channels and destinations.

The system supports ten channels. By default, channels 0 through 6 are configured with channel names and output destinations. You can change these default settings as needed. You can also configure channels 7, 8 and 9 and associate them with specific output destinations to meet your needs.

Table 2 Information channels and output destinations

Information channel number	Default channel name	Default output destination	Description
0	console	Console	Receives log, trap and debug information.
1	monitor	Monitor terminal	Receives log, trap and debug information, facilitating remote maintenance.
2	loghost	Log host	Receives log, trap and debug information and information will be stored in files for future retrieval.

Information channel number	Default channel name	Default output destination	Description
3	trapbuffer	Trap buffer	Receives trap information, a buffer inside the device for recording information.
4	logbuffer	Log buffer	Receives log information, a buffer inside the device for recording information.
5	snmpagent	SNMP module	Receives trap information.
6	channel6	Web interface	Receives log information.
7	channel7	Not specified	Receives log, trap, and debug information.
8	channel8	Not specified	Receives log, trap, and debug information.
9	channel9	Not specified	Receives log, trap, and debug information.

Outputting system information by source module

The system is composed of a variety of protocol modules, and configuration modules. You can classify, filter, and output system information based on source modules. To view the supported source modules, use the **info-center source ?** command.

Default output rules of system information

A default output rule specifies the system information source modules, information type, and severity levels for an output destination. [Table 3](#) shows the default output rules. The following describes the default settings:

- All log information is output to the Web interface. Log information with a severity level of at least informational is output to the log host, console, monitor terminal, and log buffer. Log information is not output to the trap buffer or the SNMP module.
- All trap information is output to the console, monitor terminal, log host, Web interface. Trap information with a severity level of at least informational is output to the trap buffer and SNMP module. Trap information is not output to the log buffer.
- All debug information is output to the console and monitor terminal. Debug information is not output to the log host, trap buffer, log buffer, the SNMP module, Web interface.

Table 3 Default output rules for different output destinations

Destination	Source modules	Log		Trap		Debug	
		State	Severity	State	Severity	State	Severity
Console	All supported modules	Enabled	Informational	Enabled	Debug	Enabled	Debug
Monitor terminal	All supported modules	Enabled	Informational	Enabled	Debug	Enabled	Debug
Log host	All supported modules	Enabled	Informational	Enabled	Debug	Disabled	Debug

Destination	Source modules	Log		Trap		Debug	
		State	Severity	State	Severity	State	Severity
Trap buffer	All supported modules	Disabled	Informational	Enabled	Informational	Disabled	Debug
Log buffer	All supported modules	Enabled	Informational	Disabled	Debug	Disabled	Debug
SNMP module	All supported modules	Disabled	Debug	Enabled	Informational	Disabled	Debug
Web interface	All supported modules	Enabled	Debug	Enabled	Debug	Disabled	Debug

System information formats

The following shows the original format of system information, which might be different from what you see. The actual format depends on the log resolution tool you use.

Formats

The system information format varies with output destinations, as shown in [Table 4](#).

Table 4 System information formats

Output destination	Format	Example
Console, monitor terminal, logbuffer, trapbuffer, SNMP module	timestamp sysname module/level/digest: content	%Jun 26 17:08:35:809 2011 Sysname SHELL/4/LOGIN: VTY login from 1.1.1.1
Log host	<ul style="list-style-type: none"> HP format: <PRI>timestamp Sysname %%vmodule/level /digest: source content UNICOM format: <PRI>timestamp Sysname vmodule/level/serial_number: content 	<ul style="list-style-type: none"> HP format: <189>Oct 9 14:59:04 201 MyDevice %%10SHELL/5/SHELL_LOGIN(l): VTY logged in from 192.168.1.21 UNICOM format: <ul style="list-style-type: none"> <186>Oct 13 16:48:08 2011 HP 10IFNET/2/210231a64jx073000020: log_type=port;content=Vlan-interface 1 link status is DOWN. <186>Oct 13 16:48:08 2011 HP 10IFNET/2/210231a64jx073000020: log_type=port;content=Line protocol on the interface Vlan-interface 1 is DOWN.

The closing set of angel brackets (< >), the space, the forward slash (/), and the colon (:) are all required in the above format.

Following is a detailed explanation of the fields involved in system information:

PRI (priority)

The priority is calculated by using this formula: $\text{facility} * 8 + \text{level}$, where:

- **facility** is the facility name, ranging from local0 to local7 (16 to 23 in decimal integers) and defaults to local7. It can be configured with **info-center loghost**. It is used to identify different log sources on the log host, and to query and filter logs from specific log sources.
- **level** ranges from 0 to 7. See [Table 1](#) for more information.

Note that the priority field is available only for information that is sent to the log host.

timestamp

Timestamp records the time when the system information was generated. The timestamp of the system information sent to a log host has a precision of seconds, and its format is configured with **info-center timestamp loghost** command. The timestamp of system information sent to all the other destinations has a precision of milliseconds, and its format is configured with the **info-center timestamp** command.

Table 5 Timestamp parameter description

Timestamp parameter	Description	Example
boot	Time since system startup, in the format of xxxxxx.yyyyyy, where xxxxxx represents the higher 32 bits, and yyyyyy represents the lower 32 bits. System information that is sent to all destinations except the log host supports this parameter.	%0.109391473 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. 0.109391473 is a timestamp in the boot format.
date	Current date and time of the system, in the format of Mmm dd hh:mm:ss:sss yyyy. All system information supports this parameter.	%May 30 05:36:29:579 2011 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. May 30 05:36:29:579 2011 is a timestamp in the date format.
iso	Timestamp format stipulated in ISO 8601 All system information supports this parameter.	<189>2011-05-30T06:42:44 Sysname %%10FTPD/5/FTPD_LOGIN(l): User ftp (192.168.1.23) has logged in successfully. 2011-05-30T06:42:44 is a timestamp in the iso format.
none	No timestamp is included. All system information supports this parameter.	% Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. No timestamp is included.

Timestamp parameter	Description	Example
no-year-date	Current date and time without year information. Only the system information that is sent to the log host supports this parameter.	<189>May 30 06:44:22 Sysname %%10FTPD/5/FTPD_LOGIN(l): User ftp (192.168.1.23) has logged in successfully. May 30 06:44:22 is a timestamp in the no-year-date format.

Sysname (host name or host IP address)

- If the system information is sent to a log host in the UNICOM format, and the **info-center loghost source** command is configured, the field is displayed as the IP address of the device that generates the system information.
- If the system information is sent to other destinations, or is sent to a log host in the HP format, the field is displayed as the system name of the device that generates the system information. You can use the **sysname** command to modify the system name. For more information, see *Fundamentals Command Reference*.

%% (vendor ID)

This field indicates that the information was generated by an HP device.

It exists only in system information sent to a log host in the HP format.

vv

This field identifies the version of the log, and has a value of 10.

It exists only in system information sent to a log host.

module

This field specifies the source module name. You can execute the **info-center source ?** command in system view to view the module list.

level (severity)

System information is divided into eight severity levels, from 0 to 7. See [Table 1](#) for more information about severity levels. You cannot change the system information levels generated by modules. However, you can use the **info-center source** command to control the output of system information based on severity levels.

digest

This field briefly describes the content of the system information. It contains a string of up to 32 characters.

For system information destined to the log host:

- If the character string ends with (l), the information is log information.
- If the character string ends with (t), the information is trap information.
- If the character string ends with (d), the information is debug information.

For system information destined to other destinations:

- If the timestamp starts with a percent sign (%), the information is log information.
- If the timestamp starts with a pound sign (#), the information is trap information.

- If the timestamp starts with an asterisk (*), the information is debug information.

serial number

This field indicates the serial number of the device that generates the system information. It is displayed only when the system information is sent to a log host in the format of UNICOM.

source

This optional field identifies the source of the information. It is displayed only when the system information is sent to a log host in HP format. It can take one of the following values:

- IRF member ID
- IP address of the log sender

content

This field provides the content of the system information.

FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

Information center configuration task list

Task	Remarks
Outputting system information to the console	Optional.
Outputting system information to the monitor terminal	Optional.
Outputting system information to a log host	Optional.
Outputting system information to the trap buffer	Optional.
Outputting system information to the log buffer	Optional.
Outputting system information to the SNMP module	Optional.
Outputting system information to the Web interface	Optional.
Managing security logs and the security log file	Optional.
Enabling synchronous information output	Optional.
Disabling an interface from generating link up or link down logging information	Optional.

Outputting system information to the console

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the information center.	info-center enable	Optional. Enabled by default.

Step	Command	Remarks
3. Name the channel with a specified channel number.	info-center channel <i>channel-number</i> name <i>channel-name</i>	Optional. See Table 2 for default channel names.
4. Configure an output channel for the console.	info-center console channel { <i>channel-number</i> <i>channel-name</i> }	Optional. By default, system information is output to the console through channel 0 (known as console).
5. Configure an output rule for the console.	info-center source { <i>module-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [debug { level <i>severity</i> state <i>state</i> } * log { level <i>severity</i> state <i>state</i> } * trap { level <i>severity</i> state <i>state</i> } *] *	Optional. See "Default output rules of system information."
6. Configure the timestamp format.	info-center timestamp { debugging log trap } { boot date none }	Optional. By default, the timestamp format for log, trap and debug information is date .
7. Return to user view.	quit	N/A
8. Enable system information output to the console.	terminal monitor	Optional. The default setting is enabled.
9. Enable the display of system information on the console.	<ul style="list-style-type: none"> • Enable the display of debug information on the console: terminal debugging • Enable the display of log information on the console: terminal logging • Enable the display of trap information on the console: terminal trapping 	Optional. By default, the console only displays log and trap information, and discards debug information.

Outputting system information to the monitor terminal

Monitor terminals refer to terminals that log in to the switch through the VTY user interface.

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the information center.	info-center enable	Optional. Enabled by default.
3. Name the channel with a specified channel number.	info-center channel <i>channel-number</i> name <i>channel-name</i>	Optional. See Table 2 for default channel names.

Step	Command	Remarks
4. Configure an output channel for the monitor terminal.	info-center monitor channel { <i>channel-number</i> <i>channel-name</i> }	Optional. By default, system information is output to the monitor terminal through channel 1 (known as monitor).
5. Configure an output rule for the monitor terminal.	info-center source { <i>module-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [debug { level <i>severity</i> state <i>state</i> } * log { level <i>severity</i> state <i>state</i> } * trap { level <i>severity</i> state <i>state</i> } *] *	Optional. See "Default output rules of system information."
6. Configure the timestamp format.	info-center timestamp { debugging log trap } { boot date none }	Optional. By default, the timestamp format for system information is date .
7. Return to user view.	quit	N/A
8. Enable system information output to the monitor terminal.	terminal monitor	The default setting is disabled
9. Enable the display of system information on the monitor terminal.	<ul style="list-style-type: none"> • Enable the display of debug information on the monitor terminal: terminal debugging • Enable the display of log information on the monitor terminal: terminal logging • Enable the display of trap information on the monitor terminal: terminal trapping 	Optional. By default, the monitor terminal only displays log and trap information, and discards debug information.

Outputting system information to a log host

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the information center.	info-center enable	Optional. Enabled by default.
3. Name the channel with a specified channel number.	info-center channel <i>channel-number</i> name <i>channel-name</i>	Optional. See Table 2 for default channel names.
4. Configure an output rule for the log host.	info-center source { <i>module-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [debug { level <i>severity</i> state <i>state</i> } * log { level <i>severity</i> state <i>state</i> } * trap { level <i>severity</i> state <i>state</i> } *] *	Optional. See "Default output rules of system information."

Step	Command	Remarks
5. Specify the source IP address for the log information.	info-center loghost source <i>interface-type interface-number</i>	Optional. By default, the source IP address of output log information is the primary IP address of the matching route's egress interface.
6. Configure the timestamp format for system information output to a log host.	info-center timestamp loghost { date iso no-year-date none }	Optional. date by default.
7. Set the format of the system information sent to a log host to UNICOM.	info-center format unicom	Optional. HP by default.
8. Specify a log host and configure the related output parameters.	info-center loghost { <i>host-ipv4-address</i> ipv6 <i>host-ipv6-address</i> } [port <i>port-number</i>] [dscp <i>dscp-value</i>] [channel { <i>channel-number</i> <i>channel-name</i> } facility <i>local-number</i>] *	By default, no log host is specified. If you use this command without specifying an output channel, the system uses channel 2 (loghost) by default. The value of the <i>port-number</i> argument must be the same as the value configured on the log host. Otherwise, the log host cannot receive system information.

Outputting system information to the trap buffer

The trap buffer only receives trap information, and discards log and debug information.

To output system information to the trap buffer:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the information center.	info-center enable	Optional. Enabled by default.
3. Name the channel with a specified channel number.	info-center channel <i>channel-number</i> name <i>channel-name</i>	Optional. See Table 2 for default channel names.
4. Configure an output channel for the trap buffer and specify the buffer size.	info-center trapbuffer [channel { <i>channel-number</i> <i>channel-name</i> } size <i>buffersize</i>] *	Optional. By default, system information is output to the trap buffer through channel 3 (known as trapbuffer) and the default buffer size is 256.

Step	Command	Remarks
5. Configure an output rule for the trap buffer.	info-center source { <i>module-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [debug { level <i>severity</i> state <i>state</i> } * log { level <i>severity</i> state <i>state</i> } * trap { level <i>severity</i> state <i>state</i> } *] *	Optional. See "Default output rules of system information."
6. Configure the timestamp format.	info-center timestamp { debugging log trap } { boot date none }	Optional. The timestamp format for system information is date by default.

Outputting system information to the log buffer

The log buffer only receives log information, and discards trap and debug information.

To output system information to the log buffer:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the information center.	info-center enable	Optional. Enabled by default.
3. Name the channel with a specified channel number.	info-center channel <i>channel-number</i> name <i>channel-name</i>	Optional. See Table 2 for default channel names.
4. Configure an output channel for the log buffer and specify the buffer size.	info-center logbuffer [channel { <i>channel-number</i> <i>channel-name</i> } size <i>buffersize</i>] *	Optional. By default, system information is output to the log buffer through channel 4 (known as logbuffer) and the default buffer size is 512.
5. Configure an output rule for the log buffer.	info-center source { <i>module-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [debug { level <i>severity</i> state <i>state</i> } * log { level <i>severity</i> state <i>state</i> } * trap { level <i>severity</i> state <i>state</i> } *] *	Optional. See "Default output rules of system information."
6. Configure the timestamp format.	info-center timestamp { debugging log trap } { boot date none }	Optional. The timestamp format for log, trap and debug information is date by default.

Outputting system information to the SNMP module

The SNMP module only receives trap information, and discards log and debug information.

To monitor the device running status, trap information is usually sent to the SNMP network management system (NMS). For this purpose, you must configure output of traps to the SNMP module, and set the trap sending parameters for the SNMP module. For more information about SNMP, see "Configuring SNMP."

To output system information to the SNMP module:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the information center.	info-center enable	Optional. Enabled by default.
3. Name the channel with a specified channel number.	info-center channel <i>channel-number</i> name <i>channel-name</i>	Optional. See Table 2 for default channel names.
4. Configure an output channel for the SNMP module.	info-center snmp channel { <i>channel-number</i> <i>channel-name</i> }	Optional. By default, system information is output to the SNMP module through channel 5 (known as snmpagent).
5. Configure an output rule for the SNMP module.	info-center source { <i>module-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [debug { level <i>severity</i> state <i>state</i> } * log { level <i>severity</i> state <i>state</i> } * trap { level <i>severity</i> state <i>state</i> } *] *	Optional. See "Default output rules of system information."
6. Configure the timestamp format.	info-center timestamp { debugging log trap } { boot date none }	Optional. The timestamp format for system information is date by default.

Outputting system information to the Web interface

The Web interface only receives log information, and discards trap and debug information.

This feature allows you to control whether to output system information to the Web interface and, if so, which system information can be output to the Web interface. The Web interface provides search and sorting functions. You can view system information by clicking corresponding tabs after logging in to the device through the Web interface.

To output system information to the Web interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the information center.	info-center enable	Optional. Enabled by default.
3. Name the channel with a specified channel number.	info-center channel <i>channel-number</i> name <i>channel-name</i>	Optional. See Table 2 for default channel names.
4. Configure an output channel for the Web interface.	info-center syslog channel { <i>channel-number</i> <i>channel-name</i> }	Optional. By default, system information is output to the Web interface through channel 6.

Step	Command	Remarks
5. Configure an output rule for the Web interface.	info-center source { <i>module-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [debug { level <i>severity</i> state <i>state</i> }* log { level <i>severity</i> state <i>state</i> }* trap { level <i>severity</i> state <i>state</i> }*]*	Optional. See "Default output rules of system information."
6. Configure the timestamp format.	info-center timestamp { debugging log trap } { boot date none }	Optional. The timestamp format for system information is date by default.

Managing security logs and the security log file

Security logs are very important for locating and troubleshooting network problems. Generally, security logs are output together with other logs. It is difficult to identify security logs among all logs.

To solve this problem, you can save security logs into a security log file without affecting the current log output rules.

The configuration of this feature and the management of the security log file are separate, and the security log file is managed by a privileged user. After logging in to the device, the administrator can enable the saving security logs into the security log file and configure related parameters. However, only the privileged user, known as the security log administrator, can perform operations on the security log file. The privileged user must pass AAA local authentication and log in to the device. No other users (including the system administrator) can perform operations on the security log file.

A security log administrator is a local user who is authorized by AAA to play the security log administrator role. You can authorize a security log administrator by executing the **authorization-attribute user-role security-audit** command in local user view.

The system administrator cannot view, copy, and rename the security log file. If they try, the system displays an "% Execution error" message. The system administrator can view, copy and rename other types of files.

For more information about local user and AAA local authentication, see *Security Configuration Guide*.

Saving security logs into the security log file

If this feature is enabled, the system first outputs security logs to the security log file buffer, and then saves the logs in the security log file buffer into the security log file at a specified interval (the security log administrator can also manually save security logs into the log file). After the logs are saved, the buffer is cleared immediately.

The size of the security log file is limited. When the maximum size is reached, the system deletes the oldest logs and writes new logs into the security log file. To avoid security log loss, you can set an alarm threshold for the security log file usage. When the alarm threshold is reached, the system outputs a message to inform the administrator. The administrator can log in to the device as the security log administrator and back up the security log file to prevent the loss of important data.

By default, security logs are not saved into the security log file. The parameters, such as the saving interval, the maximum size, and the alarm threshold, have default settings. To modify these parameters, log in to the device as the system administrator, and then follow the steps in the following table to configure the related parameters:

To save security logs into the security log file:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the information center.	info-center enable	Optional. Enabled by default.
3. Enable the saving of the security logs into the security log file.	info-center security-logfile enable	Disabled by default.
4. Set the interval for saving security logs to the security log file.	info-center security-logfile frequency <i>freq-sec</i>	Optional. The default saving interval is 600 seconds.
5. Set the maximum size of the security log file.	info-center security-logfile size-quota <i>size</i>	Optional. The default value is 1 MB.
6. Set the alarm threshold of the security log file usage.	info-center security-logfile alarm-threshold <i>usage</i>	Optional. The default setting is 80. When the usage of the security log file reaches 80%, the system will inform the user.

Managing the security log file

After passing the AAA local authentication, the security log administrator can perform the following operations:

Task	Command	Remarks
Display a summary of the security log file.	display security-logfile summary [{ begin exclude include } <i>regular-expression</i>]	Optional.
Change the directory where the security log file is saved.	info-center security-logfile switch-directory <i>dir-name</i>	Optional. By default, the directory to save the security log file is the seclog directory in the root directory of the storage medium. Available in user view.
Display contents of the security log file buffer.	display security-logfile buffer [{ begin exclude include } <i>regular-expression</i>]	Optional.
Save all the contents in the security log file buffer into the security log file.	security-logfile save	Optional. By default, the system automatically saves the security log file at a frequency configured by the info-center security-logfile frequency command into a directory configured by the info-center security-logfile switch-directory command. Available in user view.

Task	Command	Remarks
Perform these operations on the security log file.	<ul style="list-style-type: none"> Display the contents of the specified file: more <i>file-url</i> Display information about all files and folders: dir [<i>/all</i>] [<i>file-url</i>] Create a folder under a specified directory on the storage medium: mkdir <i>directory</i> Change the current working directory: cd { <i>directory</i> <i>..</i> <i>/</i> } Display the current path: pwd Move a specified file from a storage medium to the recycle bin: delete [<i>/unreserved</i>] <i>file-url</i> Remove a folder: rmdir <i>directory</i> Format a storage medium: format <i>device</i> Restore a file from the Recycle Bin: undelete <i>file-url</i> 	<p>Optional.</p> <p>Available in user view</p> <p>For more information about these commands, see <i>Fundamentals Command Reference</i>.</p>
	<ul style="list-style-type: none"> Establish an SFTP connection in an IPv4 network: sftp <i>server</i> [<i>port-number</i>] [<i>identity-key</i> { <i>dsa</i> <i>rsa</i> } <i>prefer-ctos-cipher</i> { <i>3des</i> <i>aes128</i> <i>des</i> } <i>prefer-ctos-hmac</i> { <i>md5</i> <i>md5-96</i> <i>sha1</i> <i>sha1-96</i> } <i>prefer-kex</i> { <i>dh-group-exchange</i> <i>dh-group1</i> <i>dh-group14</i> } <i>prefer-stoc-cipher</i> { <i>3des</i> <i>aes128</i> <i>des</i> } <i>prefer-stoc-hmac</i> { <i>md5</i> <i>md5-96</i> <i>sha1</i> <i>sha1-96</i> }] * Establish an SFTP connection in an IPv6 network: sftp <i>server</i> [<i>port-number</i>] [<i>identity-key</i> { <i>dsa</i> <i>rsa</i> } <i>prefer-ctos-cipher</i> { <i>3des</i> <i>aes128</i> <i>des</i> } <i>prefer-ctos-hmac</i> { <i>md5</i> <i>md5-96</i> <i>sha1</i> <i>sha1-96</i> } <i>prefer-kex</i> { <i>dh-group-exchange</i> <i>dh-group1</i> <i>dh-group14</i> } <i>prefer-stoc-cipher</i> { <i>3des</i> <i>aes128</i> <i>des</i> } <i>prefer-stoc-hmac</i> { <i>md5</i> <i>md5-96</i> <i>sha1</i> <i>sha1-96</i> }] * Upload a file on the client to the remote SFTP server: put <i>localfile</i> [<i>remotefile</i>] Download a file from a remote SFTP server and save it: get <i>remotefile</i> [<i>localfile</i>] For all other operations supported by the device acting as an SFTP client, see <i>Security Configuration Guide</i>. 	<p>Optional.</p> <p>The sftp commands are available in user view; the other commands are available in SFTP client view.</p> <p>For more information about these commands, see <i>Security Command Reference</i>.</p>

Enabling synchronous information output

The output of system logs interrupts ongoing configuration operations, and you have to find the previously input commands before the logs. Synchronous information output can show the previous input after log output and a command prompt in command editing mode, or a [Y/N] string in interaction mode so you can continue your operation from where you were stopped.

If system information, such as log information, is output before you input any information under the current command line prompt, the system does not display the command line prompt after the system information output.

If system information is output when you are inputting some interactive information (non Y/N confirmation information), the system displays your previous input in a new line but does not display the command line prompt.

To enable synchronous information output:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable synchronous information output.	info-center synchronous	Disabled by default

Disabling an interface from generating link up or link down logging information

By default, all interfaces generate link up or link down log information when the interface state changes. In some cases, you might want to disable specific interfaces from generating this information. For example:

- You are concerned only about the states of some interfaces. In this case, you can use this function to disable other interfaces from generating link up and link down log information.
- An interface is unstable and continuously outputs log information. In this case, you can disable the interface from generating link up and link down log information.

Use the default setting in normal cases to avoid affecting interface status monitoring.

To disable an interface from generating link up or link down logging information:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Disable the interface from generating link up or link down logging information.	undo enable log updown	By default, all interfaces generate link up and link down logging information when the interface state changes.

Enabling log file overwrite-protection

This function is available only in FIPS mode.

With log file overwrite-protection enabled, the device does not write new messages into the log file when the capacity of the log file reaches the upper limit or the storage device runs out of memory.

To enable log file overwrite protection:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable log file overwrite-protection.	info-center logfile overwrite-protection [all-port-powerdown]	By default, log file overwrite-protection is disabled.

NOTE:

With the **all-port-powerdown** keyword specified, the system shuts down all the physical ports except for the console port and physical ports that have been bound to an IRF port when the capacity of the log file reaches the upper limit or the storage device runs out of flash. To restore the device to normal state, first back up the log file and delete the original file, and then bring up the interfaces.

Displaying and maintaining information center

Task	Command	Remarks
Display the information about information channels.	display channel [<i>channel-number</i> <i>channel-name</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the information about each output destination.	display info-center [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the state of the log buffer and the log information recorded.	display logbuffer [reverse] [level <i>severity</i> size <i>buffersize</i> slot <i>slot-number</i>] * [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display a summary of the log buffer.	display logbuffer summary [level <i>severity</i> slot <i>slot-number</i>] * [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the state of the trap buffer and the trap information recorded.	display trapbuffer [reverse] [size <i>buffersize</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Clear the log buffer.	reset logbuffer	Available in user view.
Clear the trap buffer.	reset trapbuffer	Available in user view.

Information center configuration examples

Outputting log information to a UNIX log host

Network requirements

Configure the device to send ARP and IP log information that has a severity level of at least informational to the UNIX log host at 1.2.0.1/16.

Figure 18 Network diagram



Configuration procedure

Before the configuration, make sure the device and the log host can reach each other.

1. Configure the device:

Enable the information center.

```
<Sysname> system-view
```

```
[Sysname] info-center enable
```

Specify the host 1.2.0.1/16 as the log host. Use channel **loghost** to output log information (optional, **loghost** by default), and use **local4** as the logging facility.

```
[Sysname] info-center loghost 1.2.0.1 channel loghost facility local4
```

To avoid outputting unnecessary information, disable the output of log, trap, and debug information of all modules on channel **loghost**.

```
[Sysname] info-center source default channel loghost debug state off log state off trap state off
```

Configure an output rule to output to the log host ARP and IP log information that has a severity level of at least **informational**. (The source modules that are allowed to output information depend on the switch model.)

```
[Sysname] info-center source arp channel loghost log level informational state on
```

```
[Sysname] info-center source ip channel loghost log level informational state on
```

2. Configure the log host:

The following configurations were performed on SunOS 4.0 which has similar configurations to the UNIX operating systems implemented by other vendors.

a. Log in to the log host as a root user.

b. Create a subdirectory named **Device** in directory **/var/log/**, and then create file **info.log** in the **Device** directory to save logs from **Device**.

```
# mkdir /var/log/Device
```

```
# touch /var/log/Device/info.log
```

c. Edit the file **/etc/syslog.conf** and add the following contents.

```
# Device configuration messages
```

```
local4.info    /var/log/Device/info.log
```

In this configuration, **local4** is the name of the logging facility that the log host uses to receive logs. **info** is the information level. The UNIX system records the log information that has a severity of at least **informational** to the file **/var/log/Device/info.log**.

NOTE:

Be aware of the following issues while editing the file **/etc/syslog.conf**:

- Comments must be on a separate line and must begin with a pound sign (#).
 - No redundant spaces are allowed after the file name.
 - The logging facility name and the information level specified in the **/etc/syslog.conf** file must be identical to those configured on the device by using the **info-center loghost** and **info-center source** commands. Otherwise the log information might not be output properly to the log host.
-

- d. Display the process ID of **syslogd**, kill the **syslogd** process and then restart **syslogd** by using the **-r** option to make the modified configuration take effect.

```
# ps -ae | grep syslogd
147
# kill -HUP 147
# syslogd -r &
```

Now, the system can record log information into the log file.

Outputting log information to a Linux log host

Network requirements

Configure the device to send log information that has a severity level of at least informational to the Linux log host at 1.2.0.1/16.

Figure 19 Network diagram



Configuration procedure

Before the configuration, make sure the device and the PC can reach each other.

1. Configure the device:

Enable the information center.

```
<Sysname> system-view
[Sysname] info-center enable
```

Specify the host 1.2.0.1/16 as the log host. Use the channel **loghost** to output log information (optional, **loghost** by default), and use **local5** as the logging facility.

```
[Sysname] info-center loghost 1.2.0.1 channel loghost facility local5
```

To avoid outputting unnecessary information, disable the output of log, trap, and debug information of all modules on channel **loghost**.

```
[Sysname] info-center source default channel loghost debug state off log state off
trap state off
```

Configure an output rule to output to the log host the log information that has a severity level of at least **informational**.

```
[Sysname] info-center source default channel loghost log level informational state on
```

2. Configure the log host:

- a. Log in to the log host as a root user.
- b. Create a subdirectory named **Device** in directory **/var/log/**, and create file **info.log** in the **Device** directory to save logs of **Device**.

```
# mkdir /var/log/Device
# touch /var/log/Device/info.log
```

- c. Edit the file **/etc/syslog.conf** and add the following contents.

```
# Device configuration messages
local5.info    /var/log/Device/info.log
```

In this configuration, **local5** is the name of the logging facility that the log host uses to receive logs. The information level is **info**. The Linux system records the log information that has a severity level of at least **informational** to the file **/var/log/Device/info.log**.

NOTE:

Be aware of the following issues while editing the file **/etc/syslog.conf**:

- Comments must be on a separate line and must begin with a pound sign (#).
- No redundant spaces are allowed after the file name.
- The logging facility name and the information level specified in the **/etc/syslog.conf** file must be identical to those configured on the device by using the **info-center loghost** and **info-center source** commands. Otherwise the log information may not be output properly to the log host.

- d. Display the process ID of **syslogd**, kill the **syslogd** process, and restart **syslogd** by using the **-r** option to make the modified configuration take effect.

```
# ps -ae | grep syslogd
147
# kill -9 147
# syslogd -r &
```

Make sure the **syslogd** process is started with the **-r** option on the Linux log host.

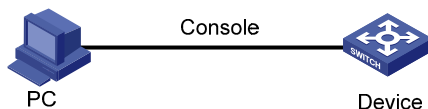
Now, the system can record log information into the log file.

Outputting log information to the console

Network requirements

Configure the device to send ARP and IP log information that has a severity level of at least **informational** to the console.

Figure 20 Network diagram



Configuration procedure

```
# Enable the information center.
```

```
<Sysname> system-view
```

```
[Sysname] info-center enable
```

Use channel **console** to output log information to the console. (This step is optional because it is the default setting.)

```
[Sysname] info-center console channel console
```

To avoid outputting unnecessary information, disable the output of log, trap, and debug information of all modules on channel **console**.

```
[Sysname] info-center source default channel console debug state off log state off trap state off
```

Configure an output rule to output to the console ARP and IP log information that has a severity level of at least **informational**. (The source modules that are allowed to output information depend on the switch model.)

```
[Sysname] info-center source arp channel console log level informational state on
```

```
[Sysname] info-center source ip channel console log level informational state on
```

```
[Sysname] quit
```

Enable the display of log information on a terminal. (Optional, this function is enabled by default.)

```
<Sysname> terminal monitor
```

Info: Current terminal monitor is on.

```
<Sysname> terminal logging
```

Info: Current terminal logging is on.

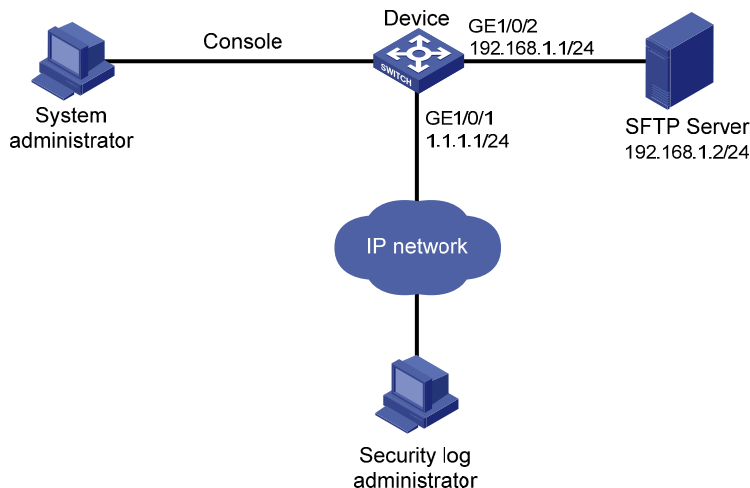
Now, if the ARP and IP modules generate log information, the information center automatically sends the log information to the console.

Saving security logs into the security log file

Network requirements

- Save security logs into the security log file **Flash:/securitylog/seclog.log** every one hour.
- Only the security log administrator can view the contents of the security log file. No other users cannot view, copy, or rename the security log file.

Figure 21 Network diagram



Configuration considerations

The configuration in this example includes two parts:

1. Log in to the device as the system administrator:
 - Enable saving the security logs into the security log file and set the saving interval to one hour.
 - Create a local user **seclog** with the password **123123123123**, and authorize this user as the security log administrator. That is, use the **authorization-attribute** command to set the user privilege level to 3 and specify the user role as security audit. In addition, specify the service types that the user can use by using **service-type**.
 - Set the authentication mode to **scheme** for the user logging in to the device, and make sure only the local user that has passed the AAA local authentication can view and perform operations on the security log file.
2. Log in to the device as the security log administrator:
 - Set the directory for saving the security log file to **Flash:/securitylog/seclog.log**.
 - View the contents of the security log file to learn the security status of the device.

Configuration procedure

1. Configuration performed by the system administrator:

Enable saving security logs into the security log file and set the saving interval to one hour.

```
<Sysname> system-view
[Sysname] info-center security-logfile enable
[Sysname] info-center security-logfile frequency 3600
```

Create a local user **seclog**, and configure the password for the user as **123123123123**.

```
[Sysname] local-user seclog
New local user added.
[Sysname-luser-seclog] password simple 123123123123
```

Authorize the user to manage the security log file.

```
[Sysname-luser-seclog] authorization-attribute level 3 user-role security-audit
```

Authorize the user to use SSH, Telnet, and terminal services.

```
[Sysname-luser-seclog] service-type ssh telnet terminal
[Sysname-luser-seclog] quit
```

According to the network plan, the user logs in to the device through SSH or Telnet, so configure the authentication mode of the VTY user interface as **scheme**.

```
[Sysname] display user-interface vty ?
    INTEGER<0-15> Specify one user terminal interface
```

The output shows that the device supports sixteen VTY user interfaces, which are numbered 0 through 15.

```
[Sysname] user-interface vty 0 15
[Sysname-ui-vty0-15] authentication-mode scheme
[Sysname-ui-vty0-15] quit
```
2. Configuration performed by the security log administrator:

Log in to the device as user **seclog**.

```
C:/> telnet 1.1.1.1
```

```
*****
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                *
* no decompiling or reverse-engineering shall be allowed.                    *
*****
```

Login authentication

Username:seclog

Password:

<Sysname>

Display the summary of the security log file.

<Sysname> display security-logfile summary

Security-log is enabled.

Security-log file size quota: 1MB

Security-log file directory: flash:/seclog

Alarm-threshold: 80%

Current usage: 0%

Writing frequency: 1 hour 0 min 0 sec

The output shows that the directory for saving the security log file is **flash:/seclog**.

Change the directory where the security log file is saved to **Flash:/securitylog**.

<Sysname> mkdir securitylog

.

%Created dir flash:/securitylog.

<Sysname> info-center security-logfile switch-directory flash:/securitylog/

Display the contents of the security log file buffer.

<Sysname> display security-logfile buffer

%@175 Nov 2 17:02:53:766 2011 Sysname SHELL/4/LOGOUT:

Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.2: logout from Console

%@176 Nov 2 17:02:53:766 2011 Sysname SHELL/5/SHELL_LOGOUT:Console logged out from aux0.

The content of other logs is not shown.

The preceding information indicates that there is still new content in the buffer that has not been saved into the security log file.

Manually save the contents of the security log file buffer into the security log file.

<Sysname> security-logfile save

Info: Save all the contents in the security log buffer into file

flash:/securitylog/seclog.log successfully.

Display the contents of the security log file.

<Sysname> more securitylog/seclog.log

%@157 Nov 2 16:12:01:750 2011 Sysname SHELL/4/LOGIN:

Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1: login from Console

%@158 Nov 2 16:12:01:750 2011 Sysname SHELL/5/SHELL_LOGIN:Console logged in from aux0.

The content of other logs is not shown.

Configuring SNMP

This chapter provides an overview of the Simple Network Management Protocol (SNMP) and guides you through the configuration procedure.

Overview

SNMP is an Internet standard protocol widely used for a management station to access and operate the devices on a network, regardless of their vendors, physical characteristics and interconnect technologies.

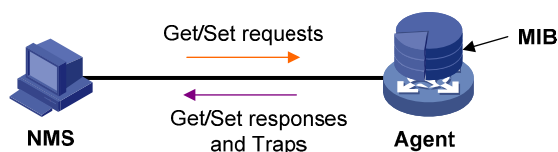
SNMP enables network administrators to read and set the variables on managed devices for state monitoring, troubleshooting, statistics collection, and other management purposes.

SNMP framework

The SNMP framework comprises the following elements:

- **SNMP manager**—Works on an NMS to monitor and manage the SNMP-capable devices in the network.
- **SNMP agent**—Works on a managed device to receive and handle requests from the NMS, and send traps to the NMS when some events, such as an interface state change, occur.
- **Management Information Base (MIB)**—Specifies the variables (for example, interface status and CPU usage) maintained by the SNMP agent for the SNMP manager to read and set.

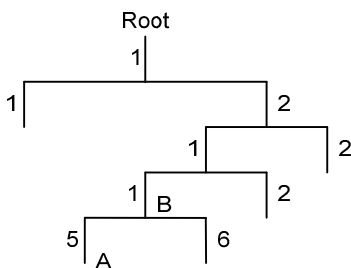
Figure 22 Relationship between an NMS, agent and MIB



MIB and view-based MIB access control

A MIB stores variables called "nodes" or "objects" in a tree hierarchy and identifies each node with a unique OID. An OID is a string of numbers that describes the path from the root node to a leaf node. For example, object B in [Figure 23](#) is uniquely identified by the OID {1.2.1.1}.

Figure 23 MIB tree



A MIB view represents a set of MIB objects (or MIB object hierarchies) with certain access privilege and is identified by a view name. The MIB objects included in the MIB view are accessible while those excluded from the MIB view are inaccessible.

A MIB view can have multiple view records each identified by a *view-name oid-tree* pair.

You control access to the MIB by assigning MIB views to SNMP groups or communities.

SNMP operations

SNMP provides the following basic operations:

- **Get**—The NMS retrieves SNMP object nodes in an agent MIB.
- **Set**—The NMS modifies the value of an object node in an agent MIB.
- **Notifications**—Includes traps and informs. SNMP agent sends traps or informs to report events to the NMS. The difference between these two types of notification is that informs require acknowledgement but traps do not. The device supports only traps.

SNMP protocol versions

HP supports SNMPv1, SNMPv2c, and SNMPv3. An NMS and an SNMP agent must use the same SNMP version to communicate with each other.

- **SNMPv1**—Uses community names for authentication. To access an SNMP agent, an NMS must use the same community name as set on the SNMP agent. If the community name used by the NMS is different from that set on the agent, the NMS cannot establish an SNMP session to access the agent or receive traps from the agent.
- **SNMPv2c**—Uses community names for authentication. SNMPv2c is compatible with SNMPv1, but supports more operation modes, data types, and error codes.
- **SNMPv3**—Uses a user-based security model (USM) to secure SNMP communication. You can configure authentication and privacy mechanisms to authenticate and encrypt SNMP packets for integrity, authenticity, and confidentiality.

SNMP configuration task list

Task	Remarks
Configuring SNMP basic parameters	Required.
Switching the NM-specific interface index format	Optional.
Configuring SNMP logging	Optional.
Configuring SNMP traps	Optional.

Configuring SNMP basic parameters

SNMPv3 differs from SNMPv1 and SNMPv2c in many ways. Their configuration procedures are described in separate sections.

Configuring SNMPv3 basic parameters

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the SNMP agent.	snmp-agent	<p>Optional.</p> <p>By default, the SNMP agent is disabled.</p> <p>You can also enable the SNMP agent by using any command that begins with snmp-agent except for the snmp-agent calculate-password and snmp-agent ifmib long-ifindex enable commands.</p>
3. Configure system information for the SNMP agent.	snmp-agent sys-info { contact <i>sys-contact</i> location <i>sys-location</i> version { all { v1 v2c v3 }* } }	<p>Optional.</p> <p>The defaults are as follows:</p> <ul style="list-style-type: none"> • Contact—null. • Location—null. • Version—SNMPv3. <p>The all, v1, and v2c keywords are supported only in non-FIPS mode.</p>
4. Configure the local engine ID.	snmp-agent local-engineid <i>engineid</i>	<p>Optional.</p> <p>The default local engine ID is the company ID plus the device ID.</p> <p>After you change the local engine ID, the existing SNMPv3 users become invalid, and you must re-create the SNMPv3 users.</p>
5. Create or update a MIB view.	snmp-agent mib-view { excluded included } <i>view-name oid-tree</i> [mask <i>mask-value</i>]	<p>Optional.</p> <p>By default, the MIB view ViewDefault is predefined and its OID is 1.</p> <p>Each <i>view-name oid-tree</i> pair represents a view record. If you specify the same record with different MIB subtree masks multiple times, the last configuration takes effect. Except the four subtrees in the default MIB view, you can create up to 16 unique MIB view records.</p>
6. Configure an SNMPv3 group.	snmp-agent group v3 <i>group-name</i> [authentication privacy] [read-view <i>read-view</i>] [write-view <i>write-view</i>] [notify-view <i>notify-view</i>] [acl <i>acl-number</i> acl ipv6 <i>ipv6-acl-number</i>] *	By default, no SNMP group exists.

Step	Command	Remarks
7. Convert a plaintext key to a ciphertext (encrypted) key.	snmp-agent calculate-password <i>plain-password mode { 3desmd5 3dessha md5 sha }</i> <i>{ local-engineid specified-engineid engineid }</i>	Optional. The 3desmd5 , 3dessha , and md5 keywords are supported only in non-FIPS mode.
8. Add a user to the SNMPv3 group.	snmp-agent usm-user v3 <i>user-name group-name [[cipher] authentication-mode { md5 sha } auth-password [privacy-mode { 3des aes128 des56 } priv-password]] [acl acl-number acl ipv6 ipv6-acl-number] *</i>	The md5 , 3des , and des56 keywords are supported only in non-FIPS mode.
9. Configure the maximum SNMP packet size (in bytes) that the SNMP agent can handle.	snmp-agent packet max-size <i>byte-count</i>	Optional. By default, the SNMP agent can receive and send SNMP packets up to 1500 bytes.
10. Configure the DSCP value for SNMP responses.	snmp-agent packet response dscp <i>dscp-value</i>	Optional. By default, the DSCP value for SNMP responses is 0.

Configuring SNMPv1 or SNMPv2c basic parameters

SNMPv1 and SNMPv2c settings are supported only in non-FIPS mode.

To configure SNMPv1 or SNMPv2c basic parameters:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the SNMP agent.	snmp-agent	Optional. By default, the SNMP agent is disabled. You can also enable the SNMP agent service by using any command that begins with snmp-agent except for the snmp-agent calculate-password and snmp-agent ifmib long-ifindex enable commands.
3. Configure system information for the SNMP agent.	snmp-agent sys-info { contact sys-contact location sys-location version { all { v1 v2c v3 }* } }	The defaults are as follows: <ul style="list-style-type: none"> • Contact—null. • Location—null. • Version—SNMPv3.
4. Configure the local engine ID.	snmp-agent local-engineid engineid	Optional. The default local engine ID is the company ID plus the device ID.

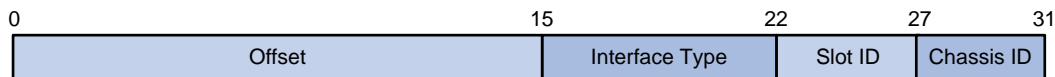
Step	Command	Remarks
		Optional. By default, the MIB view ViewDefault is predefined and its OID is 1. Each <i>view-name oid-tree</i> pair represents a view record. If you specify the same record with different MIB subtree masks multiple times, the last configuration takes effect. Except the four subtrees in the default MIB view, you can create up to 16 unique MIB view records.
5. Create or update a MIB view.	snmp-agent mib-view { excluded included } <i>view-name oid-tree</i> [mask mask-value]	
6. Configure the SNMP access right.	<ul style="list-style-type: none"> • (Method 1) Create an SNMP community: snmp-agent community { read write } <i>community-name</i> [mib-view view-name] [acl acl-number acl ipv6 ipv6-acl-number] * • (Method 2) Create an SNMP group, and add a user to the SNMP group: <ul style="list-style-type: none"> a. snmp-agent group { v1 v2c } <i>group-name</i> [read-view read-view] [write-view write-view] [notify-view notify-view] [acl acl-number acl ipv6 ipv6-acl-number] * b. snmp-agent usm-user { v1 v2c } <i>user-name group-name</i> [acl acl-number acl ipv6 ipv6-acl-number] * 	<p>Use either method.</p> <p>By default, no SNMP group exists.</p> <p>The username configured by using method 2 is equivalent to the community name configured by using method 1, and it must be the same as the community name configured on the NMS.</p>
7. Configure the maximum size (in bytes) of SNMP packets for the SNMP agent.	snmp-agent packet max-size <i>byte-count</i>	Optional. By default, the SNMP agent can receive and send the SNMP packets up to 1500 bytes.
8. Configure the DSCP value for SNMP responses.	snmp-agent packet response dscp <i>dscp-value</i>	Optional. By default, the DSCP value for SNMP responses is 0.

Switching the NM-specific interface index format

A network management (NM)-specific ifindex identifies an interface and is provided by the SNMP managed device to the NMS. A network management-specific ifindex takes one of the following two formats:

- **16-bit NM-specific ifindex**—The system dynamically assigns 16-bit NM-specific ifindex values to uniquely identify its interfaces. The 16-bit NM-specific ifindex value starts from 1 and increments by 1.
- **32-bit NM-specific ifindex**—A 32-bit NM-specific ifindex value comprises an Offset, Interface Type, Slot ID, and Chassis ID, as shown in [Figure 24](#).

Figure 24 32-bit NM-specific ifindex



- **Offset**—This field is 16 bits long and distinguishes different interfaces of the same type on the same interface card.
- **Interface type**—This field is 7 bits long and contains the enumerated value specific to the interface type. It supports up to 128 different interface types and supports more than 80 interface types at present.
- **Slot ID**—This field is 5 bits long and contains the number of the physical slot that holds the interface.
- **Chassis ID**—This field is 4 bits long. For a distributed device in IRF mode, this field indicates the IRF member ID of the device that provides the interface. For other types of devices, this field takes on 0 and is always ignored.

Configuration guidelines

- Use the 32-bit NM-specific ifindex format if the NMS requires the format to get information such as the slot that contains a specific interface. If the network protocol operating on the NMS does not support 32-bit NM-specific ifindex values, make sure NM-specific ifindex values on the device are 16-bit. By default, the device adopts the 16-bit NM-specific ifindex format.
- An NM-specific ifindex format change invalidates the NM-specific ifindex dependent settings, and these settings cannot become valid until you switch the format back. To use these settings in the new format, you must re-configure them. For example, if an RMON alarm group or private alarm group has alarm variables in the format *OID/variable-name.NM-specific-ifindex*, you must reconfigure these variables after an NM-specific ifindex format change.

Configuration procedure

To switch the NM-specific ifindex format:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Switch the format of an NM-specific ifindex from 16-bit to 32-bit.	snmp-agent ifmib long-ifindex enable	Optional. By default, an NM-specific ifindex is in 16-bit format.

Step	Command	Remarks
3. Switch the format of an NM-specific ifindex from 32-bit to 16-bit.	undo snmp-agent ifmib long-ifindex enable	Optional. By default, an NM-specific ifindex is in 16-bit format.

Configuring SNMP logging

ⓘ IMPORTANT:

Disable SNMP logging in normal cases to prevent a large amount of SNMP logs from decreasing device performance.

The SNMP logging function logs Get requests, Set requests, and Set responses, but does not log Get responses.

- **Get operation**—The agent logs the IP address of the NMS, name of the accessed node, and node OID.
- **Set operation**—The agent logs the NMS' IP address, name of accessed node, node OID, variable value, and error code and index for the Set operation.

The SNMP module sends these logs to the information center as informational messages. You can configure the information center to output these messages to certain destinations, for example, the console and the log buffer. The total output size for the node field (MIB node name) and the value field (value of the MIB node) in each log entry is 1024 bytes. If this limit is exceeded, the information center truncates the data in the fields. For more information about the information center, see "[Configuring the information center](#)."

To configure SNMP logging:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable SNMP logging.	snmp-agent log { all get-operation set-operation }	By default, SNMP logging is disabled.

Configuring SNMP traps

The SNMP agent sends traps to inform the NMS of important events, such as a reboot.

Traps include generic traps and vendor-specific traps. Generic traps include **authentication**, **coldstart**, **linkdown**, **linkup** and **warmstart**. All other traps are vendor-defined.

SNMP traps generated by a module are sent to the information center. You can configure the information center to enable or disable outputting the traps from a module by severity and set output destinations. For more information about the information center, see "[Configuring the information center](#)."

Enabling SNMP traps

Enable SNMP traps only if necessary. SNMP traps are memory-intensive and may affect device performance.

To generate linkUp or linkDown traps when the link state of an interface changes, you must enable the linkUp or linkDown trap function globally by using the **snmp-agent trap enable [standard [linkdown | linkup] *]** command and on the interface by using the **enable snmp trap updown** command.

After you enable a trap function for a module, whether the module generates traps also depends on the configuration of the module. For more information, see the configuration guide for each module.

To enable traps:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable traps globally.	snmp-agent trap enable [arp rate-limit configuration default-route flash standard [authentication coldstart linkdown linkup warmstart]* system]	By default, all traps are enabled.
3. Enter interface view.	interface <i>interface-type interface-number</i>	N/A
4. Enable link state traps.	enable snmp trap updown	By default, the link state traps are enabled.

Configuring the SNMP agent to send traps to a host

The SNMP module buffers the traps received from a module in a trap queue. You can set the size of the queue, the duration that the queue holds a trap, and trap target (destination) hosts, typically the NMS.

To successfully send traps, you must also perform the following tasks:

- Complete the basic SNMP settings and verify that they are the same as on the NMS. If SNMPv1 or SNMPv2c is used, you must configure a community name. If SNMPv3 is used, you must configure an SNMPv3 user and MIB view.
- Make sure the device and the NMS can reach each other.

To configure the SNMP agent to send traps to a host:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure a target host.	snmp-agent target-host trap address udp-domain { ip-address ipv6 ipv6-address } [udp-port port-number] [dscp dscp-value] params securityname security-string [v1 v2c v3 [authentication privacy]]	If the trap destination is a host, the <i>ip-address</i> argument must be the IP address of the host.
3. Configure the source address for traps.	snmp-agent trap source <i>interface-type interface-number</i>	Optional. By default, SNMP chooses the IP address of an interface to be the source IP address of traps.

Step	Command	Remarks
4. Extend the standard linkUp/linkDown traps.	snmp-agent trap if-mib link extended	Optional. By default, standard linkUp/linkDown traps are used. Extended linkUp/linkDown traps add interface description and interface type to standard linkUp/linkDown traps. If the NMS does not support extended SNMP messages, use standard linkUp/linkDown traps.
5. Configure the trap queue size.	snmp-agent trap queue-size <i>size</i>	Optional. The default trap queue size is 100. When the trap queue is full, the oldest traps are automatically deleted for new traps.
6. Configure the trap holding time.	snmp-agent trap life <i>seconds</i>	Optional. The default setting is 120 seconds. A trap is deleted when its holding time expires.

Displaying and maintaining SNMP

Task	Command	Remarks
Display SNMP agent system information, including the contact, physical location, and SNMP version.	display snmp-agent sys-info [contact location version] * [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display SNMP agent statistics.	display snmp-agent statistics [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the local engine ID.	display snmp-agent local-engineid [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display SNMP group information.	display snmp-agent group [<i>group-name</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display basic information about the trap queue.	display snmp-agent trap queue [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the modules that can send traps and their trap status (enable or disable).	display snmp-agent trap-list [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display SNMPv3 user information.	display snmp-agent usm-user [engineid <i>engineid</i> username <i>user-name</i> group <i>group-name</i>] * [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

Task	Command	Remarks
Display SNMPv1 or SNMPv2c community information.	display snmp-agent community [read write] [[{ begin exclude include } <i>regular-expression</i>]	Available in any view. (This command is supported only in non-FIPS mode.)
Display MIB view information.	display snmp-agent mib-view [exclude include viewname <i>view-name</i>] [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.

SNMP configuration examples

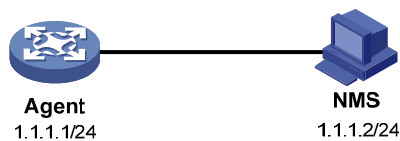
This section gives examples of how to configure SNMPv1 or SNMPv2c, SNMPv3, and SNMP logging.

SNMPv1/SNMPv2c configuration example

Network requirements

As shown in [Figure 25](#), the NMS (1.1.1.2/24) uses SNMPv1 or SNMPv2c to manage the SNMP agent (1.1.1.1/24), and the agent automatically sends traps to report events to the NMS.

Figure 25 Network diagram



Configuration procedure

1. Configure the SNMP agent:

Configure the IP address of the agent, and make sure the agent and the NMS can reach each other. (Details not shown.)

Specify SNMPv1 and SNMPv2c, and create a read-only community **public** and a read and write community **private**.

```

<Agent> system-view
[Agent] snmp-agent sys-info version v1 v2c
[Agent] snmp-agent community read public
[Agent] snmp-agent community write private
  
```

Configure contact and physical location information for the agent.

```

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

Enable SNMP traps, set the NMS at 1.1.1.2 as an SNMP trap destination, and use public as the community name. (To make sure the NMS can receive traps, specify the same SNMP version in the snmp-agent target-host command as is configured on the NMS.)

```

[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname public v1
[Agent] quit
  
```

2. Configure the SNMP NMS:

Configure the SNMP version for the NMS as v1 or v2c, create a read-only community and name it **public**, and create a read and write community and name it **private**. For information about configuring the NMS, see the NMS manual.

NOTE:

The SNMP settings on the agent and the NMS must match.

3. Verify the configuration:

Try to get the count of sent traps from the agent. The attempt succeeds.

Send request to 1.1.1.1/161 ...

Protocol version: SNMPv1

Operation: Get

Request binding:

1: 1.3.6.1.2.1.11.29.0

Response binding:

1: Oid=snmpOutTraps.0 Syntax=CNTR32 Value=18

Get finished

Use a wrong community name to get the value of a MIB node from the agent. You can see an authentication failure trap on the NMS.

1.1.1.1/2934 V1 Trap = authenticationFailure

SNMP Version = V1

Community = public

Command = Trap

Enterprise = 1.3.6.1.4.1.43.1.16.4.3.50

GenericID = 4

SpecificID = 0

Time Stamp = 8:35:25.68

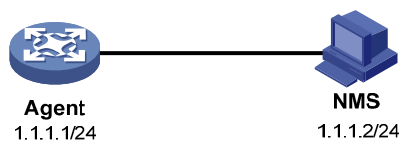
SNMPv3 configuration example

Network requirements

As shown in [Figure 26](#), the NMS (1.1.1.2/24) uses SNMPv3 to monitor and manage the interface status of the agent (1.1.1.1/24), and the agent automatically sends traps to report events to the NMS.

The NMS and the agent perform authentication when they set up an SNMP session. The authentication algorithm is MD5 and the authentication key is **authkey**. The NMS and the agent also encrypt the SNMP packets between them by using the DES algorithm and the privacy key **prikey**.

Figure 26 Network diagram



Configuration procedure

1. Configure the agent:

Configure the IP address of the agent and make sure the agent and the NMS can reach each other. (Details not shown.)

Assign the NMS read and write access to the objects under the snmp node (OID 1.3.6.1.2.1.11), and deny its access to any other MIB object.

```
<Agent> system-view
```

```
[Agent] undo snmp-agent mib-view ViewDefault
```

```
[Agent] snmp-agent mib-view included test snmp
```

```
[Agent] snmp-agent group v3 managev3group read-view test write-view test
```

Set the username to **managev3user**, authentication algorithm to **MD5**, authentication key to **authkey**, encryption algorithm to **DES56**, and privacy key to **prikey**.

```
[Agent] snmp-agent usm-user v3 managev3user managev3group authentication-mode md5  
authkey privacy-mode des56 prikey
```

Configure contact person and physical location information for the agent.

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
```

```
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

Enable traps, specify the NMS at 1.1.1.2 as a trap destination, and set the username to **managev3user** for the traps.

```
[Agent] snmp-agent trap enable
```

```
[Agent] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname  
managev3user v3 privacy
```

2. Configure the SNMP NMS:

- Specify the SNMP version for the NMS as v3.
- Create two SNMP users: **managev3user** and **public**.
- Enable both authentication and privacy functions.
- Use MD5 for authentication and DES for encryption.
- Set the authentication key to **authkey** and the privacy key to **prikey**.
- Set the timeout time and maximum number of retries.

For information about configuring the NMS, see the NMS manual.

NOTE:

The SNMP settings on the agent and the NMS must match.

3. Verify the configuration:

Try to get the count of sent traps from the agent. The get attempt succeeds.

```
Send request to 1.1.1.1/161 ...
```

```
Protocol version: SNMPv3
```

```
Operation: Get
```

```
Request binding:
```

```
1: 1.3.6.1.2.1.11.29.0
```

```
Response binding:
```

```
1: Oid=snmpOutTraps.0 Syntax=CNTR32 Value=18
```

```
Get finished
```

Try to get the device name from the agent. The get attempt fails because the NMS has no access right to the node.

```
Send request to 1.1.1.1/161 ...
```

```
Protocol version: SNMPv3
```

```
Operation: Get
```

```
Request binding:
```

```

1: 1.3.6.1.2.1.1.5.0
Response binding:
1: Oid=sysName.0 Syntax=noSuchObject Value=NULL
Get finished

# Execute the shutdown or undo shutdown command on an idle interface on the agent. You can
see the interface state change traps on the NMS:

1.1.1.1/3374 V3 Trap = linkdown
SNMP Version = V3
Community = managev3user
Command = Trap
1.1.1.1/3374 V3 Trap = linkup
SNMP Version = V3
Community = managev3user
Command = Trap

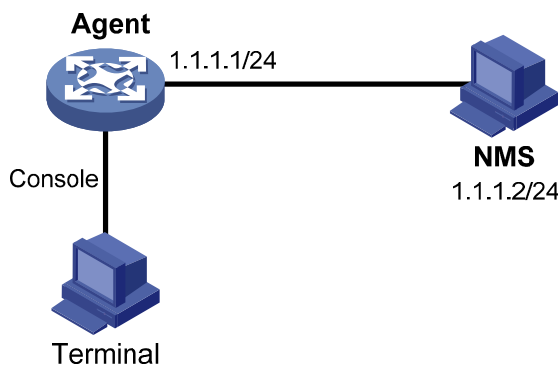
```

SNMP logging configuration example

Network requirements

Configure the SNMP agent (1.1.1.1/24) in [Figure 27](#) to log the SNMP operations performed by the NMS.

Figure 27 Network diagram



Configuration procedure

This example assumes you have configured all required SNMP settings for the NMS and the agent (see "[SNMPv1/SNMPv2c configuration example](#)" or "[SNMPv3 configuration example](#)").

Enable displaying log messages on the configuration terminal. (This function is enabled by default. Skip this step if you are using the default.)

```

<Agent> terminal monitor
<Agent> terminal logging

```

Enable the information center to output system information with severity level equal to or higher than informational to the console port.

```

<Agent> system-view
[Agent] info-center source snmp channel console log level informational

```

Enable logging GET and SET operations.

```

[Agent] snmp-agent log all

```

Verify the configuration:

Use the NMS to get a MIB variable from the agent. The following is a sample log message displayed on the configuration terminal:

```
%Jan 1 02:49:40:566 2011 Sysname SNMP/6/GET:
seqNO = <10> srcIP = <1.1.1.2> op = <get> node = <sysName(1.3.6.1.2.1.1.5.0)> value=<>
```

Use the NMS to set a MIB variable on the agent. The following is a sample log message displayed on the configuration terminal:

```
%Jan 1 02:59:42:576 2011 Sysname SNMP/6/SET:
seqNO = <11> srcIP = <1.1.1.2> op = <set> errorIndex = <0> errorStatus =<noError> node
= <sysName(1.3.6.1.2.1.1.5.0)> value = <Agent>
```

Table 6 SNMP log message field description

Field	Description
Jan 1 02:49:40:566 2011	Time when the SNMP log was generated.
seqNO	Serial number automatically assigned to the SNMP log, starting from 0.
srcIP	IP address of the NMS.
op	SNMP operation type (GET or SET).
node	MIB node name and OID of the node instance.
errorIndex	Error index, with 0 meaning no error.
errorStatus	Error status, with noError meaning no error.
value	Value set by the SET operation. This field is null for a GET operation. If the value is a character string that has invisible characters or characters beyond the ASCII range 0 to 127, the string is displayed in hexadecimal format, for example, value = <81-43>[hex].

The information center can output system event messages to several destinations, including the terminal and the log buffer. In this example, SNMP log messages are output to the terminal. To configure other message destinations, see "[Configuring the information center.](#)"

Configuring RMON

This chapter describes how to configure RMON.

Overview

Remote Monitoring (RMON) is an enhancement to SNMP for remote device management and traffic monitoring. An RMON monitor, typically the RMON agent embedded in a network device, periodically or continuously collects traffic statistics for the network attached to a port, and when a statistic crosses a threshold, logs the crossing event and sends a trap to the management station.

RMON uses SNMP traps to notify NMSs of exceptional conditions. RMON SNMP traps report various events, including traffic events such as broadcast traffic threshold exceeded. In contrast, SNMP standard traps report device operating status changes such as link up, link down, and module failure.

RMON enables proactive monitoring and management of remote network devices and subnets. The managed device can automatically send a trap when a statistic crosses an alarm threshold, and the NMS does not need to constantly poll MIB variables and compare the results. As a result, network traffic is reduced.

Working mechanism

RMON monitors typically take one of the following forms:

- **Dedicated RMON probes**—NMSs can obtain management information from RMON probes directly and control network resources. In this approach, NMSs can obtain all RMON MIB information.
- **RMON agents embedded in network devices**—NMSs exchange data with RMON agents by using basic SNMP operations to gather network management information. Because this approach is resource intensive, most RMON agent implementations provide only four groups of MIB information: alarm, event, history, and statistics.

HP devices provide the embedded RMON agent function. You can configure your device to collect and report traffic statistics, error statistics, and performance statistics.

RMON groups

Among the RFC 2819 defined RMON groups, HP implements the statistics group, history group, event group, and alarm group supported by the public MIB. HP also implements a private alarm group, which enhances the standard alarm group.

Ethernet statistics group

The statistics group defines that the system collects traffic statistics on interfaces (only Ethernet interfaces are supported) and saves the statistics in the Ethernet statistics table (ethernetStatsTable). The interface traffic statistics include network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, and packets received.

After you create a statistics entry for an interface, the statistics group starts to collect traffic statistics on the interface. The statistics in the Ethernet statistics table are cumulative sums.

History group

The history group defines that the system periodically collects traffic statistics on interfaces and saves the statistics in the history record table (ethernetHistoryTable). The statistics include bandwidth utilization, number of error packets, and total number of packets.

The history statistics table record traffic statistics collected for each sampling interval. The sampling interval is user-configurable.

Event group

The event group defines event indexes and controls the generation and notifications of the events triggered by the alarms defined in the alarm group and the private alarm group. The events can be handled in one of the following ways:

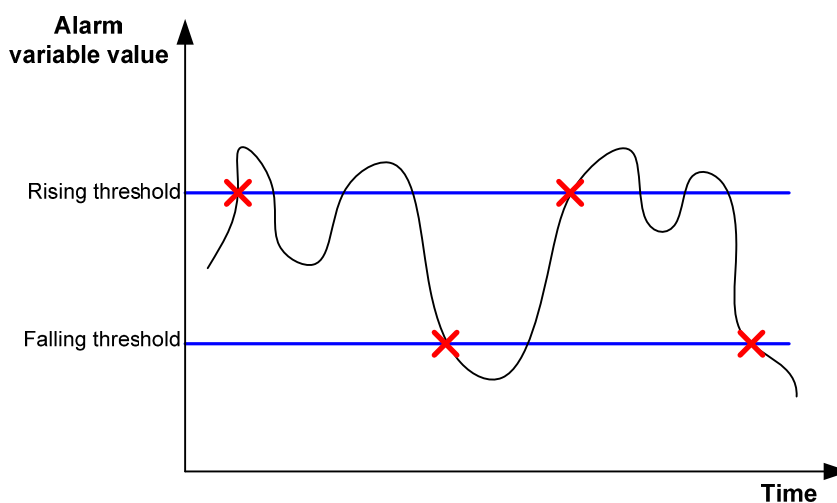
- **Log**—Logs event information (including event name and description) in the event log table of the RMON MIB, so the management device can get the logs through the SNMP Get operation.
- **Trap**—Sends a trap to notify an NMS of the event.
- **Log-Trap**—Logs event information in the event log table and sends a trap to the NMS.
- **None**—No action.

Alarm group

The RMON alarm group monitors alarm variables, such as the count of incoming packets (etherStatsPkts) on an interface. After you define an alarm entry, the system gets the value of the monitored alarm variable at the specified interval. If the value of the monitored variable is greater than or equal to the rising threshold, a rising event is triggered. If the value of the monitored variable is smaller than or equal to the falling threshold, a falling event is triggered. The event is then handled as defined in the event group.

If an alarm entry crosses a threshold multiple times in succession, the RMON agent generates an alarm event only for the first crossing. For example, if the value of a sampled alarm variable crosses the rising threshold multiple times before it crosses the falling threshold, only the first crossing triggers a rising alarm event, as shown in [Figure 28](#).

Figure 28 Rising and falling alarm events



Private alarm group

The private alarm group calculates the values of alarm variables and compares the results with the defined threshold for a more comprehensive alarming function.

The system handles the private alarm entry (as defined by the user) in the following ways:

- Periodically samples the private alarm variables defined in the private alarm formula.
- Calculates the sampled values based on the private alarm formula.
- Compares the result with the defined threshold and generates an appropriate event if the threshold value is reached.

If a private alarm entry crosses a threshold multiple times in succession, the RMON agent generates an alarm event only for the first crossing. For example, if the value of a sampled alarm variable crosses the rising threshold multiple times before it crosses the falling threshold, only the first crossing triggers a rising alarm event. If the count result of the private alarm group overpasses the same threshold multiple times, only the first one can cause an alarm event. In other words, the rising alarm and falling alarm are alternate.

Configuring the RMON statistics function

The RMON statistics function can be implemented by either the Ethernet statistics group or the history group, but the objects of the statistics are different, as follows:

- A statistics object of the Ethernet statistics group is a variable defined in the Ethernet statistics table, and the recorded content is a cumulative sum of the variable from the time the statistics entry is created to the current time. For more information, see ["Configuring the RMON Ethernet statistics function."](#)
- A statistics object of the history group is the variable defined in the history record table, and the recorded content is a cumulative sum of the variable in each period. For more information, see ["Configuring the RMON history statistics function."](#)

Configuring the RMON Ethernet statistics function

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Create an entry in the RMON statistics table.	rmon statistics <i>entry-number</i> [owner <i>text</i>]	N/A

You can create one statistics entry per interface and up to 100 statistics entries on the device. When the number of statistics entries exceeds 100, you cannot add new entries.

Configuring the RMON history statistics function

Follow these guidelines when you configure the RMON history statistics function:

- The *entry-number* for an RMON history control entry must be globally unique. If an entry number has been used on one interface, it cannot be used on another.

- You can configure multiple history control entries for one interface, but must make sure their entry numbers and sampling intervals are different.
- The device supports up to 100 history control entries.
- You can successfully create a history control entry, even if the specified bucket size exceeds the history table size supported by the device. However, the effective bucket size will be the actual value supported by the device.

To configure the RMON history statistics function:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Create an entry in the RMON history control table.	rmon history <i>entry-number</i> buckets <i>number</i> interval <i>sampling-interval</i> [owner <i>text</i>]	N/A

Configuring the RMON alarm function

Follow these guidelines when you configure the RMON alarm function:

- To send traps to the NMS when an alarm is triggered, configure the SNMP agent as described in "Configuring SNMP" before configuring the RMON alarm function.
- If the alarm variable is a MIB variable defined in the history group or the Ethernet statistics group, make sure the RMON Ethernet statistics function or the RMON history statistics function is configured on the monitored Ethernet interface. Otherwise, even if you can create the alarm entry, no alarm event can be triggered.
- You cannot create a new event, alarm, or private alarm entry that has the same set of parameters as an existing entry. For parameters to be compared for duplication, see [Table 7](#).
- After the maximum number of entries is reached, no new entry can be created. For the table entry limits, see [Table 7](#).

To configure the RMON alarm function:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an event entry in the event table.	rmon event <i>entry-number</i> [description <i>string</i>] { log log-trap <i>log-trapcommunity</i> none trap <i>trap-community</i> } [owner <i>text</i>]	N/A

Step	Command	Remarks
3. Create an entry in the alarm table or private alarm table.	<ul style="list-style-type: none"> Create an entry in the alarm table: rmon alarm <i>entry-number alarm-variable sampling-interval</i> { absolute delta } rising-threshold <i>threshold-value1 event-entry1</i> falling-threshold <i>threshold-value2 event-entry2</i> [owner <i>text</i>] Create an entry in the private alarm table: rmon prialarm <i>entry-number prialarm-formula prialarm-des sampling-interval</i> { absolute changeratio delta } rising-threshold <i>threshold-value1 event-entry1</i> falling-threshold <i>threshold-value2 event-entry2</i> entrytype { forever cycle <i>cycle-period</i> } [owner <i>text</i>] 	Use at least one command.

Table 7 RMON configuration restrictions

Entry	Parameters to be compared	Maximum number of entries
Event	Event description (description <i>string</i>), event type (log , trap , logtrap or none) and community name (<i>trap-community</i> or <i>log-trapcommunity</i>)	60
Alarm	Alarm variable (<i>alarm-variable</i>), sampling interval (<i>sampling-interval</i>), sampling type (absolute or delta), rising threshold (<i>threshold-value1</i>) and falling threshold (<i>threshold-value2</i>)	60
Prialarm	Alarm variable formula (<i>alarm-variable</i>), sampling interval (<i>sampling-interval</i>), sampling type (absolute , changeratio or delta), rising threshold (<i>threshold-value1</i>) and falling threshold (<i>threshold-value2</i>)	50

Displaying and maintaining RMON

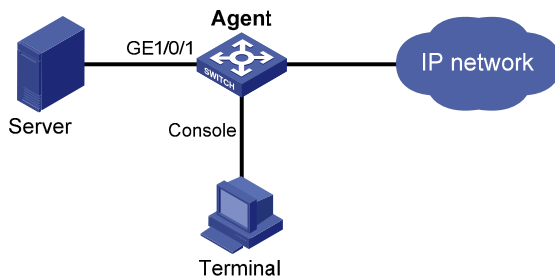
Task	Command	Remarks
Display RMON statistics.	display rmon statistics [<i>interface-type interface-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the RMON history control entry and history sampling information.	display rmon history [<i>interface-type interface-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display RMON alarm configuration.	display rmon alarm [<i>entry-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display RMON private alarm configuration.	display rmon prialarm [<i>entry-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display RMON event configuration.	display rmon event [<i>entry-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display log information for event entries.	display rmon eventlog [<i>entry-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

Ethernet statistics group configuration example

Network requirements

Configure the RMON statistics group on the RMON agent in [Figure 29](#) to gather cumulative traffic statistics for GigabitEthernet 1/0/1.

Figure 29 Network diagram



Configuration procedure

Configure the RMON statistics group on the RMON agent to gather statistics for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1 owner user1
```

Display statistics collected by the RMON agent for GigabitEthernet 1/0/1.

```
<Sysname> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by user1-rmon is VALID.
Interface : GigabitEthernet1/0/1<ifIndex.3>
etherStatsOctets      : 21657      , etherStatsPkts      : 307
etherStatsBroadcastPkts : 56      , etherStatsMulticastPkts : 34
etherStatsUndersizePkts : 0      , etherStatsOversizePkts : 0
etherStatsFragments   : 0      , etherStatsJabbers     : 0
etherStatsCRCAlignErrors : 0      , etherStatsCollisions  : 0
etherStatsDropEvents (insufficient resources): 0
Packets received according to length:
64      : 235      , 65-127 : 67      , 128-255 : 4
256-511: 1      , 512-1023: 0      , 1024-1518: 0
```

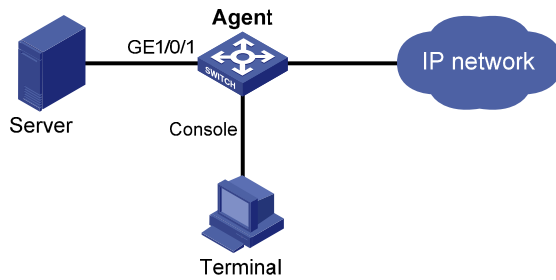
On the configuration terminal, get the traffic statistics through SNMP. (Details not shown.)

History group configuration example

Network requirements

Configure the RMON history group on the RMON agent in [Figure 30](#) to gather periodical traffic statistics for GigabitEthernet 1/0/1 every one minute.

Figure 30 Network diagram



Configuration procedure

Configure the RMON history group on the RMON agent to gather traffic statistics every one minute for GigabitEthernet 1/0/1. Retain up to eight records for the interface in the history statistics table.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon history 1 buckets 8 interval 60 owner user1
```

Display the history data collected for GigabitEthernet 1/0/1.

```
[Sysname-GigabitEthernet1/0/1] display rmon history
HistoryControlEntry 2 owned by null is VALID
  Samples interface      : GigabitEthernet1/0/1<ifIndex.3>
  Sampling interval      : 10(sec) with 8 buckets max
  Sampled values of record 1 :
    dropevents           : 0                , octets                : 834
    packets               : 8                , broadcast packets        : 1
    multicast packets     : 6                , CRC alignment errors    : 0
    undersize packets     : 0                , oversize packets        : 0
    fragments             : 0                , jabbers                  : 0
    collisions            : 0                , utilization               : 0
  Sampled values of record 2 :
    dropevents           : 0                , octets                : 962
    packets               : 10               , broadcast packets        : 3
    multicast packets     : 6                , CRC alignment errors    : 0
    undersize packets     : 0                , oversize packets        : 0
    fragments             : 0                , jabbers                  : 0
    collisions            : 0                , utilization               : 0
  Sampled values of record 3 :
    dropevents           : 0                , octets                : 830
    packets               : 8                , broadcast packets        : 0
    multicast packets     : 6                , CRC alignment errors    : 0
    undersize packets     : 0                , oversize packets        : 0
    fragments             : 0                , jabbers                  : 0
    collisions            : 0                , utilization               : 0
  Sampled values of record 4 :
    dropevents           : 0                , octets                : 933
    packets               : 8                , broadcast packets        : 0
    multicast packets     : 7                , CRC alignment errors    : 0
    undersize packets     : 0                , oversize packets        : 0
```

```

    fragments      : 0          , jabbers      : 0
    collisions     : 0          , utilization : 0
Sampled values of record 5 :
    dropevents     : 0          , octets     : 898
    packets        : 9          , broadcast packets : 2
    multicast packets : 6        , CRC alignment errors : 0
    undersize packets : 0        , oversize packets : 0
    fragments      : 0          , jabbers      : 0
    collisions     : 0          , utilization : 0
Sampled values of record 6 :
    dropevents     : 0          , octets     : 898
    packets        : 9          , broadcast packets : 2
    multicast packets : 6        , CRC alignment errors : 0
    undersize packets : 0        , oversize packets : 0
    fragments      : 0          , jabbers      : 0
    collisions     : 0          , utilization : 0
Sampled values of record 7 :
    dropevents     : 0          , octets     : 766
    packets        : 7          , broadcast packets : 0
    multicast packets : 6        , CRC alignment errors : 0
    undersize packets : 0        , oversize packets : 0
    fragments      : 0          , jabbers      : 0
    collisions     : 0          , utilization : 0
Sampled values of record 8 :
    dropevents     : 0          , octets     : 1154
    packets        : 13         , broadcast packets : 1
    multicast packets : 6        , CRC alignment errors : 0
    undersize packets : 0        , oversize packets : 0
    fragments      : 0          , jabbers      : 0
    collisions     : 0          , utilization : 0

```

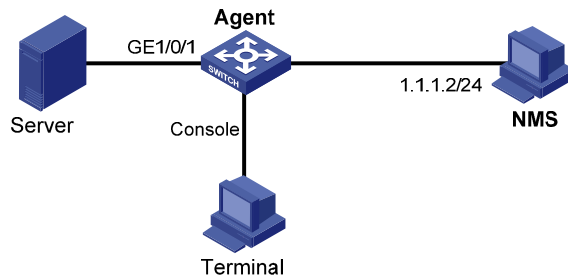
On the configuration terminal, get the traffic statistics through SNMP. (Details not shown.)

Alarm group configuration example

Network requirements

Configure the RMON alarm group on the RMON agent in [Figure 31](#) to send alarms in traps when the five-second incoming traffic statistic on GigabitEthernet 1/0/1 crosses the rising threshold or drops below the falling threshold.

Figure 31 Network diagram



Configuration procedure

Configure the SNMP agent with the same SNMP settings as the NMS at 1.1.1.2. This example uses SNMPv1, read community **public**, and write community **private**.

```
<Sysname> system-view
[Sysname] snmp-agent
[Sysname] snmp-agent community read public
[Sysname] snmp-agent community write private
[Sysname] snmp-agent sys-info version v1
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname public
```

Configure the RMON statistics group to gather traffic statistics for GigabitEthernet 1/0/1.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1 owner user1
[Sysname-GigabitEthernet1/0/1] quit
```

Create an RMON event entry and an RMON alarm entry so the RMON agent sends traps when the delta sampling value of node 1.3.6.1.2.1.16.1.1.1.4.1 exceeds 100 or drops below 50.

```
[Sysname] rmon event 1 trap public owner user1
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 5 delta rising-threshold 100 1
falling-threshold 50 1
```

Display the RMON alarm entry configuration.

```
<Sysname> display rmon alarm 1
AlarmEntry 1 owned by null is Valid.
  Samples type           : delta
  Variable formula       : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval      : 5(sec)
  Rising threshold       : 100(linked with event 1)
  Falling threshold      : 50(linked with event 2)
  When startup enables   : risingOrFallingAlarm
  Latest value           : 0
```

Display statistics for GigabitEthernet 1/0/1.

```
<Sysname> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by user1-rmon is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets      : 57329      , etherStatsPkts      : 455
  etherStatsBroadcastPkts : 53      , etherStatsMulticastPkts : 353
```

```

etherStatsUndersizePkts : 0          , etherStatsOversizePkts : 0
etherStatsFragments      : 0          , etherStatsJabbers      : 0
etherStatsCRCAlignErrors : 0          , etherStatsCollisions   : 0
etherStatsDropEvents (insufficient resources): 0
Packets received according to length:
64      : 7          , 65-127 : 413          , 128-255 : 35
256-511: 0          , 512-1023: 0          , 1024-1518: 0

```

Query alarm events on the NMS. (Details not shown.)

On the RMON agent, alarm event messages are displayed when events occur. The following is a sample output:

```

[Sysname]
#Jan 27 16:31:34:12 2011 Sysname RMON/2/ALARMFALL:Trap 1.3.6.1.2.1.16.0.2 Alarm table 1
monitors 1.3.6.1.2.1.16.1.1.1.4.1 with sample type 2,has sampled alarm value 0 less than(or
=) 50.

```

Configuring port mirroring

Introduction to port mirroring

Port mirroring is the process of copying the packets passing through a port to the monitor port connecting to a monitoring device for packet analysis.

Terminologies of port mirroring

Mirroring source

The mirroring source can be one or more monitored ports. Packets (called "mirrored packets") passing through them are copied to a port connecting to a monitoring device for packet analysis. Such a port is called a "source port" and the device where the port resides is called a "source device".

Mirroring destination

The mirroring destination is the destination port (also known as the monitor port) of mirrored packets and connects to the data monitoring device. The device where the monitor port resides is called the "destination device." The monitor port forwards mirrored packets to its connected monitoring device.

A monitor port may receive multiple duplicates of a packet in some cases because it can monitor multiple mirroring sources. For example, assume that Port 1 is monitoring bidirectional traffic on Port 2 and Port 3 on the same device. If a packet travels from Port 2 to Port 3, two duplicates of the packet will be received on Port 1.

Mirroring direction

The mirroring direction indicates that the inbound, outbound, or bidirectional traffic can be copied on a mirroring source.

- Inbound: Copies packets received on a mirroring source.
- Outbound: Copies packets sent out of a mirroring source.
- Bidirectional: Copies packets both received and sent on a mirroring source.

Mirroring group

Port mirroring is implemented through mirroring groups, which fall into local, remote source, and remote destination mirroring groups. For more information about the mirroring groups, see "[Port mirroring classification and implementation](#)."

Reflector port, egress port, and remote probe VLAN

The reflector port, remote probe VLAN, and egress port are used for Layer 2 remote port mirroring. The remote probe VLAN specially transmits mirrored packets to the destination device. Both the reflector port and egress port reside on a source device and send mirrored packets to the remote probe VLAN. The egress port must belong to the remote probe VLAN while the reflector port may not. For more information about the source device, destination device, reflector port, egress port, and remote probe VLAN, see "[Port mirroring classification and implementation](#)."

NOTE:

The reflector port is used to enable local mirroring to support multiple monitor ports.

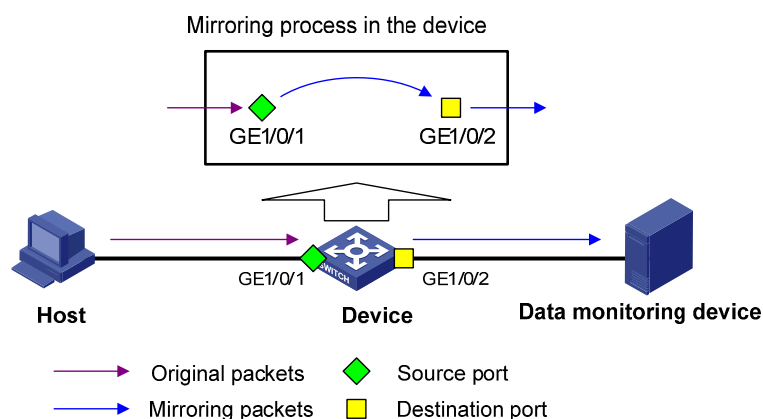
Port mirroring classification and implementation

According to the locations of the mirroring source and the mirroring destination, port mirroring falls into local port mirroring and remote port mirroring.

Local port mirroring

In local port mirroring, the mirroring source and the mirroring destination are on the same device. A mirroring group that contains the mirroring source and the mirroring destination on the device is called a "local mirroring group".

Figure 32 Local port mirroring implementation



As shown in [Figure 32](#), the source port GigabitEthernet 1/0/1 and monitor port GigabitEthernet 1/0/2 reside on the same device. Packets of GigabitEthernet 1/0/1 are copied to GigabitEthernet 1/0/2, which then forwards the packets to the data monitoring device for analysis.

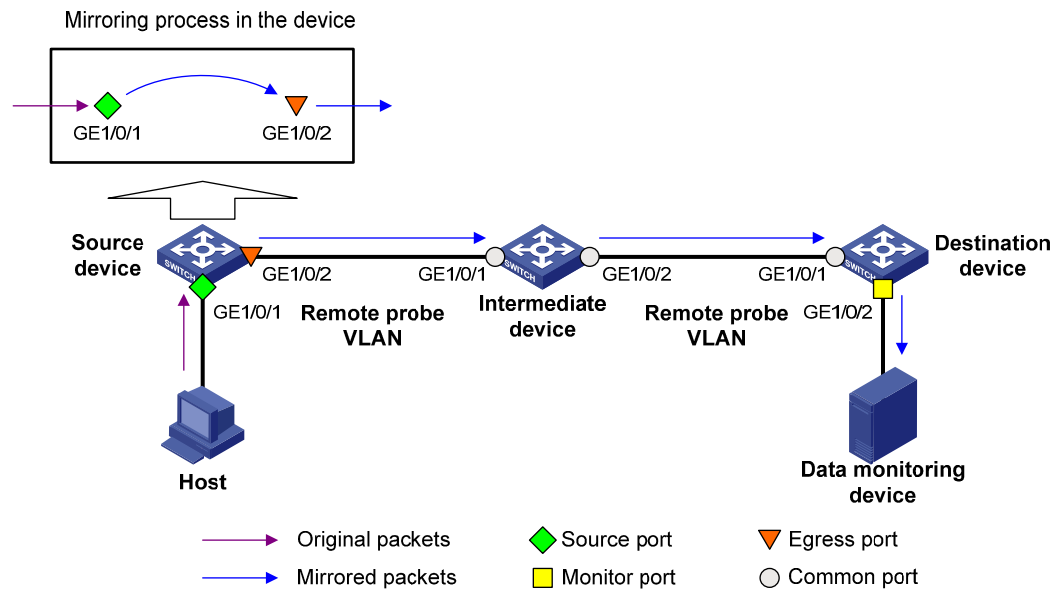
Remote port mirroring

In remote port mirroring, the mirroring source and the mirroring destination reside on different devices and in different mirroring groups. The mirroring group that contains the mirroring source or the mirroring destination is called a "remote source/destination group". The devices between the source devices and destination device are intermediate devices.

Because the source and destination devices are on the same Layer 2 network, remote port mirroring is also referred to Layer 2 remote port mirroring.

1. Layer 2 remote port mirroring

Figure 33 Layer 2 remote port mirroring implementation



On the network shown in [Figure 33](#),

The source device does the following:

2. Copies the packets received on the source port GigabitEthernet 1/0/1 to the egress port GigabitEthernet 1/0/2.
3. Forwards the packets to the intermediate device, which then broadcasts the packets in the remote probe VLAN.
4. Transmits the packets to the destination device via the intermediate device.

Then, the destination device does the following:

5. Receives the mirrored packets.
6. Compares their VLAN IDs to the ID of the remote probe VLAN configured in the remote destination group.
7. If the VLAN IDs of these mirrored packets match the remote probe VLAN ID, the device forwards them to the data monitoring device through the monitor port GigabitEthernet 1/0/2.

Allow remote probe VLAN to pass through the intermediate devices to make sure the source device and the destination device can communicate at Layer 2 in the remote probe VLAN.

For a mirrored packet to successfully arrive at the remote destination device, make sure the VLAN ID of the mirrored packet is not removed or changed. Otherwise, the Layer 2 remote port mirroring configuration will fail.

To monitor both the received and sent packets of a port in a mirroring group, you must use the **mac-address mac-learning disable** command on the source, intermediate, and destination devices to disable MAC address learning of the remote probe VLAN. For more information about the **mac-address mac-learning disable** command, see *Layer 2—LAN Switch Command Reference*.

Configuring local port mirroring

Local port mirroring configuration task list

Configure a local mirroring group and then configure one or more source ports and a monitor port for the local mirroring group.

Complete these tasks to configure local port mirroring:

Task	Remarks
Creating a local mirroring group	Required.
Configuring source ports for the local mirroring group	Required
Configuring the monitor port for the local mirroring group	Required.
Using the remote probe VLAN to enable local mirroring to support multiple monitor ports	Optional.

Creating a local mirroring group

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a local mirroring group.	mirroring-group <i>group-id</i> local	No local mirroring group exists by default.

NOTE:

A local mirroring group takes effect only after you configure a monitor port and source ports for it.

Configuring source ports for the local mirroring group

If you use system view, you can use a list to configure multiple source ports for a mirroring group at one time. If you use interface view, you can assign only the current port to the group as a source port, so you must repeat the step for each additional port.

Configuration restrictions and guidelines

- A mirroring group can contain multiple source ports.
- A port can belong to only one mirroring group.

Configuring source ports in system view

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure source ports.	mirroring-group <i>group-id</i> mirroring-port <i>mirroring-port-list</i> { both inbound outbound }	By default, no source port is configured for a local mirroring group.

Configuring a source port in interface view

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the current port as a source port.	[mirroring-group <i>group-id</i>] mirroring-port { both inbound outbound }	By default, a port does not serve as a source port for any local mirroring group.

Configuring the monitor port for the local mirroring group

You can configure the monitor port for a mirroring group in system view, or assign the current port to a mirroring group as the monitor port in interface view. The two methods lead to the same result.

Configuration restrictions and guidelines

- A mirroring group contains only one monitor port.
- To make sure that the mirroring function works properly, do not assign the monitor port to a source VLAN, or enable the spanning tree feature on the monitor port.
- HP recommends you use a monitor port for port mirroring only. This is to make sure that the data monitoring device receives and analyzes only the mirrored traffic rather than a mix of mirrored traffic and normally forwarded traffic.
- You cannot configure the monitor port in a mirroring group as a port in a RRPP ring.

Configuring the monitor port in system view

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the monitor port.	mirroring-group <i>group-id</i> monitor-port <i>monitor-port-id</i>	By default, no monitor port is configured for a local mirroring group.

Configuring the monitor port in interface view

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the current port as the monitor port.	[mirroring-group <i>group-id</i>] monitor-port	By default, a port does not serve as the monitor port for any local mirroring group.

Using the remote probe VLAN to enable local mirroring to support multiple monitor ports

In typical local port mirroring configuration, you can configure only one monitor port in a local mirroring group. As a result, you cannot monitor traffic of a local device on multiple data monitoring devices. To do that, you can take advantage of the remote probe VLAN used in Layer 2 remote mirroring.

In Layer 2 remote port mirroring, a remote probe VLAN is configured, and the mirrored packets are broadcast within the remote probe VLAN. By connecting multiple data monitoring devices to the member ports of the remote probe VLAN, you can monitor the traffic of the local device on multiple data monitoring devices.

Configure this feature in the following steps:

1. Configure a remote source mirroring group on the local device
2. Configure the monitored ports on the device as source ports of this mirroring group
3. Configure a remote probe VLAN for this mirroring group
4. Assign the ports connecting the data monitoring devices to the remote probe VLAN

In this way, when packets mirrored on the monitored ports are broadcast in the remote probe VLAN, they will be sent out of the ports connecting the data monitoring devices, and all the data monitoring devices can thus receive these mirrored packets.

Configuration restrictions and guidelines

- The reflector port of a remote source mirroring group must be an access port and belong to the default VLAN, VLAN 1.
- HP recommends that you configure an unused port as the reflector port of a remote source mirroring group and disable STP on it.
- Do not configure a combo interface as a reflector port.
- A mirroring group can contain multiple source ports.
- To make sure that the port mirroring function works properly, do not assign a source port to the remote probe VLAN.
- If you have already configured a reflector port for a remote source mirroring group, you can no longer configure an egress port for it.
- A VLAN can serve as the remote probe VLAN for only one remote source mirroring group. HP recommends you use the remote probe VLAN for port mirroring exclusively. Do not create a VLAN interface for the VLAN or configure any other features for the VLAN.
- A remote probe VLAN must be a static VLAN. To remove the VLAN configured as a remote probe VLAN, you must first remove the remote probe VLAN with the **undo mirroring-group remote-probe vlan** command.
- If the remote probe VLAN of a remote mirroring group is removed, the remote mirroring group will become invalid.
- The link type of monitor ports configured for port mirroring must be access.

Configuration procedure

To configure local port mirroring with multiple monitor ports:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a remote source mirroring group.	mirroring-group <i>group-id</i> remote-source	By default, no mirroring group exists on a device.
3. Configure source ports for the remote source mirroring group.	<ul style="list-style-type: none"> (Method 1) In system view: mirroring-group <i>group-id</i> mirroring-port <i>mirroring-port-list</i> { both inbound outbound } (Method 2) In interface view: a. interface <i>interface-type</i> <i>interface-number</i> b. [mirroring-group <i>group-id</i>] mirroring-port { both inbound outbound } c. quit 	Use either method. By default, no source port is configured for a mirroring group.
4. Configure the reflector port for the remote source mirroring group.	mirroring-group <i>group-id</i> reflector-port <i>reflector-port</i>	By default, no reflector port is configured for a mirroring group.
5. Create the remote probe VLAN and enter VLAN view.	vlan <i>vlan-id</i>	By default, no remote probe VLAN is configured for a mirroring group.
6. Assign monitor ports to the remote probe VLAN.	port <i>interface-list</i>	By default, a newly-created VLAN does not have any member port.
7. Return to system view.	quit	N/A
8. Configure the remote probe VLAN for the remote source mirroring group.	mirroring-group <i>group-id</i> remote-probe vlan <i>rprobe-vlan-id</i>	By default, no remote probe VLAN is configured for a mirroring group.

Configuring Layer 2 remote port mirroring

Layer 2 remote port mirroring configuration task list

Configuring Layer 2 remote port mirroring is to configure remote mirroring groups. To do that, configure the remote source group on the source device and configure the cooperating remote destination group on the destination device. If an intermediate device exists, allow the remote probe VLAN to pass through the intermediate device.

NOTE:

HP recommends you not enable GARP VLAN Registration Protocol (GVRP). If GVRP is enabled, GVRP may register the remote probe VLAN to unexpected ports, resulting in undesired duplicates. For more information about GVRP, see *Layer 2—LAN Switching Configuration Guide*.

Then, configure the following on the destination device:

- Remote probe VLAN
- Monitor port

Configure the following on the source device:

- Source ports
- Remote probe VLAN
- The egress port

Complete these tasks to configure Layer 2 remote port mirroring:

Task	Remarks
Configuring a remote destination group	Creating a remote destination group Required.
	Configuring the monitor port for the remote destination group Required.
	Configuring the remote probe VLAN for the remote destination group Required.
	Assigning the monitor port to the remote probe VLAN Required.
Configuring a remote source group	Creating a remote source group Required.
	Configuring source ports for the remote source group Required.
	Configuring the egress port for the remote source group Required.
	Configuring the remote probe VLAN for the remote source group Required.

Configuring a remote destination group (on the destination device)

To configure a remote destination group, make the following configurations on the destination device:

Creating a remote destination group

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a remote destination group.	mirroring-group <i>group-id</i> remote-destination	By default, no remote destination group exists on a device.

Configuring the monitor port for the remote destination group

You can configure the monitor port for a mirroring group in system view, or assign the current port to a mirroring group as the monitor port in interface view. The two methods lead to the same result.

1. Configuration restrictions and guidelines:

- A mirroring group contains only one monitor port.
- To make sure that the mirroring function works properly, do not enable the spanning tree feature on the monitor port.
- HP recommends you use a monitor port only for port mirroring. This is to make sure that the data monitoring device receives and analyzes only the mirrored traffic rather than a mix of mirrored traffic and normally forwarded traffic.
- You cannot configure the monitor port in a mirroring group as a port in a RRPP ring.

2. Configuration procedure:

To configure the monitor port for the remote destination group in system view:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the monitor port.	mirroring-group <i>group-id</i> monitor-port <i>monitor-port-id</i>	By default, no monitor port is configured for a remote destination group.

To configure the monitor port for the remote destination group in interface view:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the current port as the monitor port.	[mirroring-group <i>group-id</i>] monitor-port	By default, a port does not serve as the monitor port for any remote destination group.

Configuring the remote probe VLAN for the remote destination group

- Configuration restrictions and guidelines:
 - A VLAN can serve for only one mirroring group.
 - When a VLAN is configured as a remote probe VLAN, use the remote probe VLAN for port mirroring exclusively. Do not configure a VLAN interface for the VLAN or configure any other features for the VLAN.
 - When a VLAN is configured as a remote probe VLAN, you must remove the remote probe VLAN configuration before deleting the VLAN.
 - When you remove the configuration of a remote probe VLAN, an active mirroring group becomes inactive.
- Configuration procedure:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the remote probe VLAN.	mirroring-group <i>group-id</i> remote-probe vlan <i>rprobe-vlan-id</i>	By default, no remote probe VLAN is configured for a remote destination group.

Assigning the monitor port to the remote probe VLAN

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter the interface view of the monitor port.	interface <i>interface-type</i> <i>interface-number</i>	N/A

Step	Command	Remarks
3. Assign the port to the probe VLAN.	<ul style="list-style-type: none"> For an access port: port access vlan <i>vlan-id</i> For a trunk port: port trunk permit vlan <i>vlan-id</i> For a hybrid port: port hybrid vlan <i>vlan-id</i> { tagged untagged } 	Use one of the commands.

For more information about the **port access vlan**, **port trunk permit vlan**, and **port hybrid vlan** commands, see *Layer 2—LAN Switching Command Reference*.

Configuring a remote source group (on the source device)

Creating a remote source group

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a remote source group.	mirroring-group <i>group-id</i> remote-source	By default, no remote source group exists on a device.

Configuring source ports for the remote source group

If you use system view, you can use a list to configure multiple source ports for a mirroring group at one time. If you use interface view, you can assign only the current port to the group as a source port, so you must repeat the step for each additional port.

- Configuration restrictions and guidelines:
 - A mirroring group can contain multiple source ports.
 - To make sure that the mirroring function works properly, do not assign a source port to the remote probe VLAN.
 - A port can belong to only one mirroring group.

- Configuration procedure:

To configure source ports for the remote source group in system view:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure source ports for the remote source group.	mirroring-group <i>group-id</i> mirroring-port <i>mirroring-port-list</i> { both inbound outbound }	By default, no source port is configured for a remote source group.

To configure a source port for the remote source group in interface view:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A

Step	Command	Remarks
3. Configure the current port as a source port.	[mirroring-group <i>group-id</i>] mirroring-port { both inbound outbound }	By default, a port does not serve as a source port for any remote source group.

Configuring the egress port for the remote source group

You can configure the egress port for a mirroring group in system view, or assign the current port to it as the egress port in interface view. The two configuration modes lead to the same result.

To make sure that the mirroring function works properly, disable these functions on the egress port: the spanning tree feature, 802.1X, IGMP snooping, static ARP, and MAC address learning.

To configure the egress port for the remote source group in system view:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the egress port for the remote source group.	mirroring-group <i>group-id</i> monitor-egress <i>monitor-egress-port</i>	By default, no egress port is configured for a remote source group.

To configure the egress port for the remote source group in interface view:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the current port as the egress port.	mirroring-group <i>group-id</i> monitor-egress	By default, a port does not serve as the egress port for any remote source group.

NOTE:

- A mirroring group contains only one egress port.
- A source port of an existing mirroring group cannot be configured as an egress port.

Configuring the remote probe VLAN for the remote source group

Before configuring a remote probe VLAN, create a static VLAN that will serve as the remote probe VLAN for the remote source group.

1. Configuration restrictions and guidelines:
 - A VLAN can serve for only one mirroring group.
 - When a VLAN is configured as a remote probe VLAN, you must remove the remote probe VLAN configuration before deleting the VLAN.
 - When you remove the configuration of a remote probe VLAN, an active mirroring group becomes inactive.
 - When a VLAN is configured as a remote probe VLAN, use the remote probe VLAN for port mirroring exclusively. Do not create a VLAN interface for the VLAN or configure any other features for the VLAN.

- The remote mirroring groups on the source device and destination device must use the same remote probe VLAN.
2. Configuration procedure:
- To configure the remote probe VLAN for the remote source group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the remote probe VLAN.	mirroring-group <i>group-id</i> remote-probe vlan <i>rprobe-vlan-id</i>	By default, no remote probe VLAN is configured for a remote source group.

Displaying and maintaining port mirroring

Task	Command	Remarks
Display the configuration of mirroring groups.	display mirroring-group { <i>group-id</i> all local remote-destination remote-source } [{ begin exclude include } <i>regular-expression</i>]	Available in any view

Port mirroring configuration examples

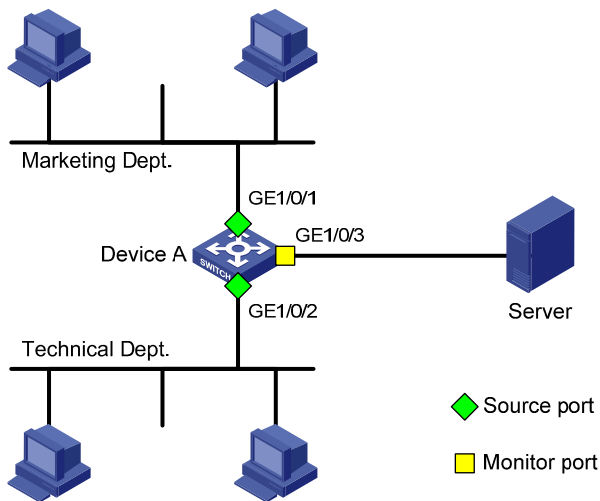
Local port mirroring configuration example

Network requirements

On the network shown in [Figure 34](#):

- Device A connects to the marketing department through GigabitEthernet 1/0/1 and to the technical department through GigabitEthernet 1/0/2. It connects to the server through GigabitEthernet 1/0/3.
- Configure local port mirroring in source port mode to enable the server to monitor the bidirectional traffic of the marketing department and the technical department.

Figure 34 Network diagram



Configuration procedure

1. Create a local mirroring group:

Create local mirroring group 1.

```
<DeviceA> system-view
```

```
[DeviceA] mirroring-group 1 local
```

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as source ports and port GigabitEthernet 1/0/3 as the monitor port.

```
[DeviceA] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2 both
```

```
[DeviceA] mirroring-group 1 monitor-port GigabitEthernet 1/0/3
```

Disable the spanning tree feature on the monitor port GigabitEthernet 1/0/3.

```
[DeviceA] interface GigabitEthernet 1/0/3
```

```
[DeviceA-GigabitEthernet1/0/3] undo stp enable
```

```
[DeviceA-GigabitEthernet1/0/3] quit
```

2. Verify the configurations:

Display the configuration of all mirroring groups.

```
[DeviceA] display mirroring-group all
```

```
mirroring-group 1:
```

```
type: local
```

```
status: active
```

```
mirroring port:
```

```
GigabitEthernet1/0/1 both
```

```
GigabitEthernet1/0/2 both
```

```
monitor port: GigabitEthernet1/0/3
```

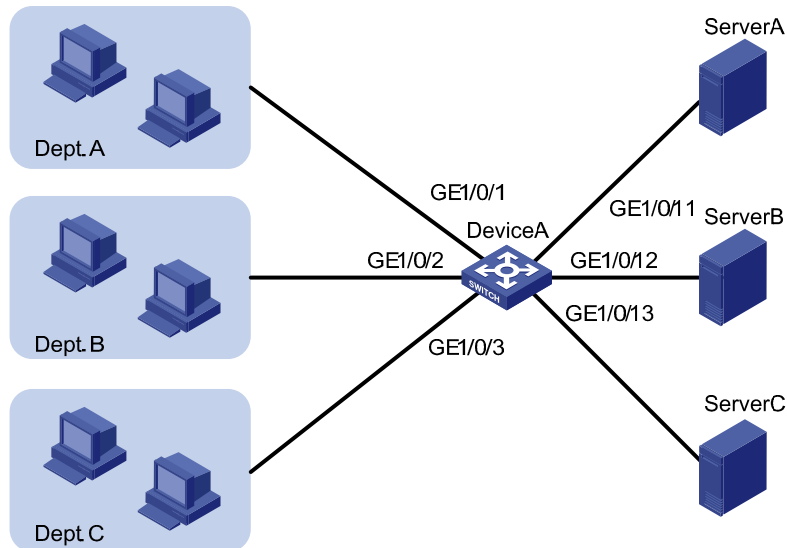
After the configurations are completed, you can monitor all the packets received and sent by the marketing department and the technical department on the server.

Local port mirroring with multiple monitor ports configuration example

Network requirements

As shown in Figure 35, Dept. A, Dept. B, and Dept. C are connected to Device A through ports GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3, respectively. Configure port mirroring to enable all three data monitoring devices, Server A, Server B, and Server C, to monitor both the incoming and outgoing traffic of the three departments.

Figure 35 Network diagram



Configuration procedure

Create remote source mirroring group 1.

```
<DeviceA> system-view
[DeviceA] mirroring-group 1 remote-source
```

Configure GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 as source ports of remote source mirroring group 1.

```
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 to gigabitethernet 1/0/3 both
```

Configure an unused port (GigabitEthernet 1/0/5 for example) of Device A as the reflector port of remote source mirroring group 1.

```
[DeviceA] mirroring-group 1 reflector-port GigabitEthernet 1/0/5
```

Create VLAN 10 and assign the three ports (GigabitEthernet 1/0/11 through GigabitEthernet 1/0/13) connecting the three data monitoring devices to VLAN 10.

```
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/11 to gigabitethernet 1/0/13
[DeviceA-vlan10] quit
```

Configure VLAN 10 as the remote probe VLAN of remote source mirroring group 1.

```
[DeviceA] mirroring-group 1 remote-probe vlan 10
```

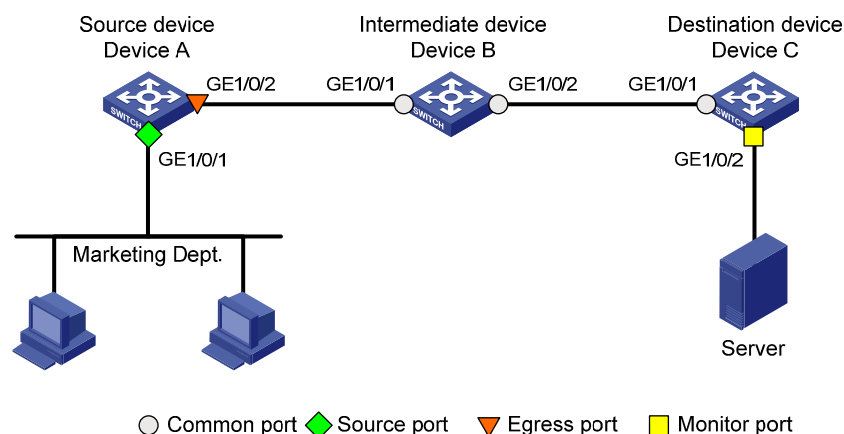
Layer 2 remote port mirroring configuration example

Network requirements

On the Layer 2 network shown in Figure 36:

- Device A connects to the marketing department through GigabitEthernet 1/0/1 and connects to the trunk port GigabitEthernet 1/0/1 of Device B through the trunk port GigabitEthernet 1/0/2. Device C connects to the server through GigabitEthernet 1/0/2 and connects to the trunk port GigabitEthernet 1/0/2 of Device B through the trunk port GigabitEthernet 1/0/1.
- Configure Layer 2 remote port mirroring to enable the server to monitor the bidirectional traffic of the marketing department.

Figure 36 Network diagram



Configuration procedure

1. Configure Device C (the destination device):

Configure GigabitEthernet 1/0/1 as a trunk port that permits the packets of VLAN 2 to pass through.

```
<DeviceC> system-view
[DeviceC] interface GigabitEthernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 2
[DeviceC-GigabitEthernet1/0/1] quit
```

Create a remote destination group.

```
[DeviceC] mirroring-group 1 remote-destination
```

Create VLAN 2 as the remote probe VLAN.

```
[DeviceC] vlan 2
```

Disable MAC address learning for the remote probe VLAN.

```
[DeviceC-vlan2] mac-address mac-learning disable
[DeviceC-vlan2] quit
```

Configure VLAN 2 as the remote probe VLAN of the mirroring group and GigabitEthernet 1/0/2 as the monitor port of the mirroring group, disable the spanning tree feature on GigabitEthernet 1/0/2, and assign the port to VLAN 2.

```
[DeviceC] mirroring-group 1 remote-probe vlan 2
[DeviceC] interface GigabitEthernet 1/0/2
```

```
[DeviceC-GigabitEthernet1/0/2] mirroring-group 1 monitor-port
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port access vlan 2
[DeviceC-GigabitEthernet1/0/2] quit
```

2. Configure Device B (the intermediate device):

Create VLAN 2 as the remote probe VLAN.

```
<DeviceB> system-view
[DeviceB] vlan 2
```

Disable MAC address learning for the remote probe VLAN.

```
[DeviceB-vlan2] mac-address mac-learning disable
[DeviceB-vlan2] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port that permits the packets of VLAN 2 to pass through.

```
[DeviceB] interface GigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port that permits the packets of VLAN 2 to pass through.

```
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface GigabitEthernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2
[DeviceB-GigabitEthernet1/0/2] quit
```

3. Configure Device A (the source device):

Create a remote source group.

```
<DeviceA> system-view
[DeviceA] mirroring-group 1 remote-source
```

Create VLAN 2 as the remote probe VLAN.

```
[DeviceA] vlan 2
```

Disable MAC address learning for the remote probe VLAN.

```
[DeviceA-vlan2] mac-address mac-learning disable
[DeviceA-vlan2] quit
```

Configure VLAN 2 as the remote probe VLAN of the mirroring group. Configure GigabitEthernet 1/0/1 as a source port and GigabitEthernet 1/0/2 as the egress port in the mirroring group.

```
[DeviceA] mirroring-group 1 remote-probe vlan 2
[DeviceA] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 both
[DeviceA] mirroring-group 1 monitor-egress GigabitEthernet 1/0/2
```

Configure output port GigabitEthernet 1/0/2 as a trunk port to permit the packets of VLAN 2 to pass through, and disable the spanning tree feature on the port.

```
[DeviceA] interface GigabitEthernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

4. Verify the configurations.

After the configurations are completed, you can monitor all the packets received and sent by the marketing department on the server.

Configuring traffic mirroring

Introduction to traffic mirroring

Traffic mirroring copies the specified packets to the specified destination for packet analyzing and monitoring. It is implemented through QoS policies. In other words, you define traffic classes and configure match criteria to classify packets to be mirrored and then configure traffic behaviors to mirror packets that fit the match criteria to the specified destination. Traffic mirroring allows you to flexibly classify packets by defining match criteria and obtain accurate statistics.

You can configure the traffic to be mirrored to an interface, to a CPU, or to a VLAN.

- Mirroring traffic to an interface copies the matching packets to a destination interface.
- Mirroring traffic to a CPU copies the matching packets to a CPU (the CPU of the device where ports with traffic mirroring configured reside).

For more information about QoS policies, traffic classes, and traffic behaviors, see *ACL and QoS Configuration Guide*.

Traffic mirroring configuration task list

Task		Remarks
Configuring match criteria		Required.
Configuring traffic mirroring of different types	Mirroring traffic to a port	Required.
	Mirroring traffic to the CPU	Perform at least one configuration.
Configuring a QoS policy		Required.
Applying a QoS policy	Apply a QoS policy to a port	Required.
	Apply a QoS policy to a VLAN	
	Apply a QoS policy globally	Perform one of these configurations.
	Apply a QoS policy to the control plane	

Configuring match criteria

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a class and enter class view.	traffic classifier <i>tcl-name</i> [operator { and or }]	By default, no traffic class exists.
3. Configure match criteria.	if-match <i>match-criteria</i>	By default, no match criterion is configured in a traffic class.

For more information about the **traffic classifier** and **if-match** commands, see *ACL and QoS Command Reference*.

Configuring traffic mirroring of different types

In a traffic behavior, you can configure only one type of traffic mirroring.

Mirroring traffic to a port

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a behavior and enter behavior view.	traffic behavior <i>behavior-name</i>	By default, no traffic behavior exists. For more information about the traffic behavior command, see <i>ACL and QoS Command Reference</i> .
3. Specify the destination interface for traffic mirroring.	mirror-to interface <i>interface-type</i> <i>interface-number</i>	By default, traffic mirroring is not configured in a traffic behavior. You can specify up to four destination interfaces by executing the mirror-to interface command repeatedly.

Mirroring traffic to the CPU

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a behavior and enter behavior view.	traffic behavior <i>behavior-name</i>	By default, no traffic behavior exists. For more information about the traffic behavior command, see <i>ACL and QoS Command Reference</i> .
3. Mirror traffic to the CPU.	mirror-to cpu	By default, no traffic mirroring is configured in a traffic behavior.

NOTE:

The CPU refers to the CPU of the device where ports with traffic mirroring configured reside.

Configuring a QoS policy

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a policy and enter policy view.	qos policy <i>policy-name</i>	By default, no policy exists.
3. Associate a class with a traffic behavior in the QoS policy.	classifier <i>tcl-name</i> behavior <i>behavior-name</i>	By default, no traffic behavior is associated with a class.

For more information about the **qos policy** and **classifier behavior** commands, see *ACL and QoS Command Reference*.

Applying a QoS policy

For more information about applying a QoS policy, see *ACL and QoS Configuration Guide*.

Apply a QoS policy to a port

By applying a QoS policy to an interface, you can mirror the traffic in a specific direction on the interface. A policy can be applied to multiple interfaces, but in one direction (inbound or outbound) of an interface, only one policy can be applied.

To apply a QoS policy to a port:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view or port group view.	<ul style="list-style-type: none">Enter interface view: interface <i>interface-type</i> <i>interface-number</i>Enter port group view: port-group manual <i>port-group-name</i>	Use either command. Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.
3. Apply a policy to the interface, all ports in the port group, or the PVC.	qos apply policy <i>policy-name</i> { inbound outbound }	For more information about the qos apply policy command, see <i>ACL and QoS Command Reference</i> .

Apply a QoS policy to a VLAN

You can apply a QoS policy to a VLAN to mirror the traffic in a specific direction on all ports in the VLAN.

To apply the QoS policy to a VLAN:

Step	Command
1. Enter system view.	system-view
2. Apply a QoS policy to a VLAN.	qos vlan-policy <i>policy-name</i> vlan <i>vlan-id-list</i> { inbound outbound }

For more information about the **qos vlan-policy** command, see *ACL and QoS Command Reference*.

Apply a QoS policy globally

You can apply a QoS policy globally to mirror the traffic in a specific direction on all ports.

To apply a QoS policy globally:

Step	Command
1. Enter system view.	system-view

Step	Command
2. Apply a QoS policy globally.	qos apply policy <i>policy-name</i> global { inbound outbound }

For more information about the **qos apply policy** command, see *ACL and QoS Command Reference*.

Apply a QoS policy to the control plane

You can apply a QoS policy to the control plane to mirror the traffic in the inbound direction of the control plane.

To apply a QoS policy to the control plane:

Step	Command
1. Enter system view.	system-view
2. Enter control plane view.	control-plane slot <i>slot-number</i>
3. Apply a QoS policy to the control plane.	qos apply policy <i>policy-name</i> inbound

For more information about the **control-plane** and **qos apply policy** commands, see *ACL and QoS Command Reference*.

Displaying and maintaining traffic mirroring

Task	Command	Remarks
Display user-defined traffic behavior configuration information.	display traffic behavior user-defined [<i>behavior-name</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display user-defined QoS policy configuration information.	display qos policy user-defined [<i>policy-name</i> [<i>classifier tcl-name</i>]] [{ begin exclude include } <i>regular-expression</i>]	Available in any view

For more information about the **display traffic behavior** and **display qos policy** commands, see *ACL and QoS Command Reference*.

Traffic mirroring configuration example

Traffic mirroring configuration example

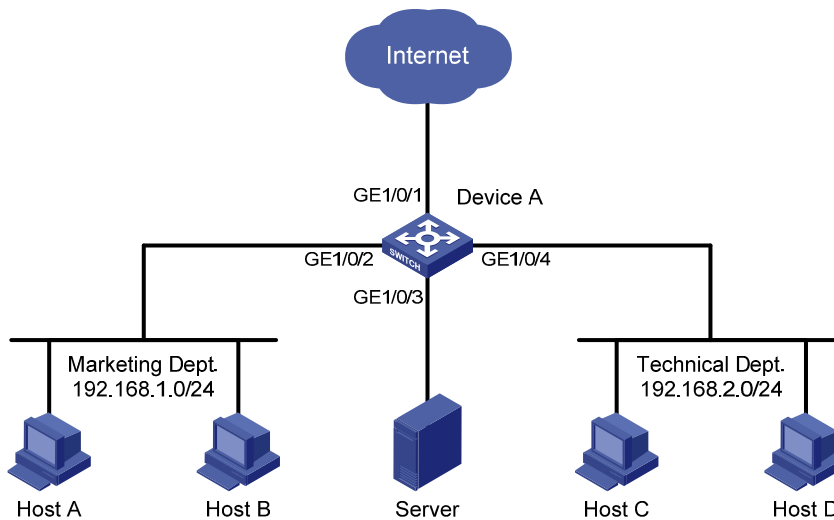
Network requirements

As shown in [Figure 37](#):

- Different departments of a company use IP addresses on different subnets. The marketing and technology departments use the IP addresses on subnets 192.168.1.0/24 and 192.168.2.0/24 respectively. The working hour of the company is from 8:00 to 18:00 on weekdays.

- Configure traffic mirroring so that the server can monitor the traffic that the technology department sends to access the Internet, and IP traffic that the technology department sends to the marketing department.

Figure 37 Network diagram



Configuration procedure

- Monitor the traffic sent by the technology department to access the Internet:
 # Create ACL 3000 to allow packets from the technology department (on subnet 192.168.2.0/24) to access the Internet.

```
<DeviceA> system-view
[DeviceA] acl number 3000
[DeviceA-acl-adv-3000] rule permit tcp source 192.168.2.0 0.0.0.255 destination-port eq www
[DeviceA-acl-adv-3000] quit
```

 # Create traffic class **tech_c**, and configure the match criterion as ACL 3000.

```
[DeviceA] traffic classifier tech_c
[DeviceA-classifier-tech_c] if-match acl 3000
[DeviceA-classifier-tech_c] quit
```

 # Create traffic behavior **tech_b**, and configure the action of mirroring traffic to port GigabitEthernet 1/0/3.

```
[DeviceA] traffic behavior tech_b
[DeviceA-behavior-tech_b] mirror-to interface GigabitEthernet 1/0/3
[DeviceA-behavior-tech_b] quit
```

 # Create QoS policy **tech_p**, and associate traffic class **tech_c** with traffic behavior **tech_b** in the QoS policy.

```
[DeviceA] qos policy tech_p
[DeviceA-qospolicy-tech_p] classifier tech_c behavior tech_b
[DeviceA-qospolicy-tech_p] quit
```

 # Apply QoS policy **tech_p** to the outgoing packets of GigabitEthernet 1/0/1.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] qos apply policy tech_p outbound
[DeviceA-GigabitEthernet1/0/1] quit
```

2. Monitor the traffic that the technology department sends to the marketing department:

Configure a time range named **work** to cover the time from 8: 00 to 18: 00 in working days.

```
[DeviceA] time-range work 8:0 to 18:0 working-day
```

Create ACL 3001 to allow packets sent from the technology department (on subnet 192.168.2.0/24) to the marketing department (on subnet 192.168.1.0/24).

```
[DeviceA] acl number 3001
```

```
[DeviceA-acl-adv-3001] rule permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255 time-range work
```

```
[DeviceA-acl-adv-3001] quit
```

Create traffic class **mkt_c**, and configure the match criterion as ACL 3001.

```
[DeviceA] traffic classifier mkt_c
```

```
[DeviceA-classifier-mkt_c] if-match acl 3001
```

```
[DeviceA-classifier-mkt_c] quit
```

Create traffic behavior **mkt_b**, and configure the action of mirroring traffic to port GigabitEthernet 1/0/3.

```
[DeviceA] traffic behavior mkt_b
```

```
[DeviceA-behavior-mkt_b] mirror-to interface GigabitEthernet 1/0/3
```

```
[DeviceA-behavior-mkt_b] quit
```

Create QoS policy **mkt_p**, and associate traffic class **mkt_c** with traffic behavior **mkt_b** in the QoS policy.

```
[DeviceA] qos policy mkt_p
```

```
[DeviceA-qospolicy-mkt_p] classifier mkt_c behavior mkt_b
```

```
[DeviceA-qospolicy-mkt_p] quit
```

Apply QoS policy **mkt_p** to the outgoing packets of GigabitEthernet 1/0/2.

```
[DeviceA] interface GigabitEthernet 1/0/2
```

```
[DeviceA-GigabitEthernet1/0/2] qos apply policy mkt_p outbound
```

3. Verify the configurations.

After completing the configurations, through the server, you can monitor all traffic sent by the technology department to access the Internet and the IP traffic that the technology department sends to the marketing department during working hours.

Configuring NQA

Overview

Network Quality Analyzer (NQA) can perform various types of tests and collect network performance and service quality parameters such as delay jitter, time for establishing a TCP connection, time for establishing an FTP connection, and file transfer rate.

With the NQA test results, you can diagnose and locate network faults, be aware of network performance in time and take proper actions to correct any problems.

NQA features

Supporting multiple test types

Ping uses only the Internet Control Message Protocol (ICMP) to test the reachability of the destination host and the round-trip time. As an enhancement to ping, NQA supports more test types and functions.

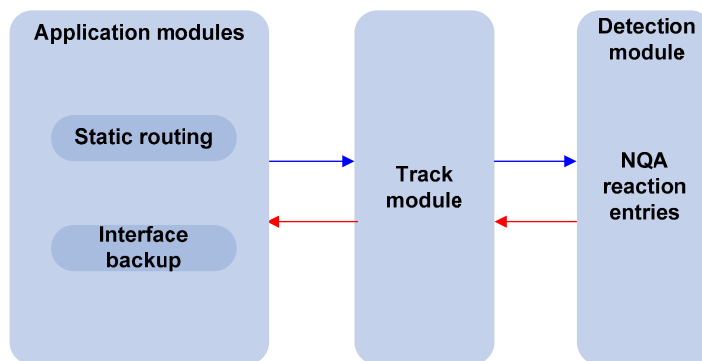
NQA supports 11 test types: ICMP echo, DHCP, DNS, FTP, HTTP, UDP jitter, SNMP, TCP, UDP echo, voice, and DLSw.

NQA enables the client to send probe packets of different test types to detect the protocol availability and response time of the peer. Test results help you understand network performance.

Supporting the collaboration function

Collaboration is implemented by establishing reaction entries to monitor the detection results of NQA probes. If the number of consecutive probe failures reaches a limit, NQA informs the track module of the detection result, and the track module triggers other application modules to take predefined.

Figure 38 Implement collaboration



The collaboration comprises the following parts: the application modules, the track module, and the detection modules.

- A detection module monitors objects, such as the link status, and network performance, and informs the track module of detection results.
- Upon the detection results, the track module changes the status of the track entry and informs the associated application module. The track module works between the application modules and the detection modules. It hides the differences among detection modules from application modules.

- The application module takes actions when the tracked object changes its state.

The following describes how a static route is monitored through collaboration.

1. NQA monitors the reachability to 192.168.0.88.
2. When 192.168.0.88 becomes unreachable, NQA notifies the track module of the change.
3. The track module notifies the state change to the static routing module
4. The static routing module sets the static route as invalid.

For more information about collaboration and the track module, see *High Availability Configuration Guide*.

Supporting threshold monitoring

NQA supports threshold monitoring for performance parameters such as average delay jitter and packet round-trip time. The performance parameters to be monitored are monitored elements. NQA monitors threshold violations for a monitored element, and reacts to certain measurement conditions (for example, sending trap messages to the network management server). This helps network administrators understand the network service quality and network performance.

- Monitored elements

[Table 8](#) describes the monitored elements and the NQA test types in which the elements can be monitored.

Table 8 Monitored elements and NQA test types

Monitored elements	Test type supported
Probe duration	Tests excluding UDP jitter test and voice test
Count of probe failures	Tests excluding UDP jitter test and voice test
Packet round-trip time	UDP jitter test and voice test
Count of discarded packets	UDP jitter test and voice test
One-way delay jitter (source-to-destination and destination-to-source)	UDP jitter test and voice test
One-way delay (source-to-destination and destination-to-source)	UDP jitter test and voice test
Calculated Planning Impairment Factor (ICPIF) (see " Configuring voice tests ")	Voice test
Mean Opinion Scores (MOS) (see " Configuring voice tests ")	Voice test

- Threshold types

The following threshold types are supported:

- **average**—Monitors the average value of monitored data in a test. If the average value in a test exceeds the upper threshold or goes below the lower threshold, a threshold violation occurs. For example, you can monitor the average probe duration in a test.
- **accumulate**—Monitors total number of times the monitored data violates the threshold in a test. If the total number of times reaches or exceeds a specific value, a threshold violation occurs.
- **consecutive**—Monitors the number of consecutive times the monitored data violates the threshold since the test group starts. If the monitored data violates the threshold consecutively for a specific number of times, a threshold violation occurs.

The counting for the average or accumulate threshold type is performed per test, but the counting for the consecutive type is performed after the test group starts.

- Triggered actions

The following actions may be triggered:

- **none**—NQA only records events for terminal display. It does not send trap information to the network management server. NQA DNS tests do not support the action of sending trap messages. The action to be triggered in DNS tests can only be the default one, **none**.
- **trap-only**—NQA records events and sends trap messages to the network management server.

- Reaction entry

In a reaction entry, a monitored element, a threshold type, and the action to be triggered are configured to implement threshold monitoring.

The state of a reaction entry can be invalid, over-threshold, or below-threshold, using the following workflow:

- Before an NQA test group starts, the reaction entry is in the state of invalid.
- After each test or probe, threshold violations are counted according to the threshold type and range configured in the entry. If the threshold is violated consecutively or accumulatively for a specific number of times, the state of the entry is set to over-threshold. Otherwise, the state of the entry is set to below-threshold.

If the action to be triggered is configured as **trap-only** for a reaction entry, when the state of the entry changes, a trap message is generated and sent to the network management server.

NQA concepts

Test group

An NQA test group specifies test parameters including the test type, destination address, and destination port. Each test group is uniquely identified by an administrator name and operation tag. You can configure and schedule multiple NQA test groups to test different objects.

Test and probe

After the NQA test group starts, tests are performed at a specific interval. During each test, a specific number of probe operations are performed. Both the test interval and the number of probe operations per test are configurable. But only one probe operation is performed during one voice test.

In different test types, probe operation has the following different meanings:

- During a TCP or DLSw test, one probe operation means setting up one connection.
- During a UDP jitter or a voice test, one probe operation means continuously sending a specific number of probe packets. The number of probe packets is configurable.
- During an FTP, HTTP, DHCP, or DNS test, one probe operation means uploading or downloading a file, obtaining a web page, obtaining an IP address through DHCP, or translating a domain name to an IP address.
- During an ICMP echo or UDP echo test, one probe operation means sending an ICMP echo request or a UDP packet.
- During an SNMP test, one probe operation means sending one SNMPv1 packet, one SNMPv2C packet, and one SNMPv3 packet.

NQA client and server

A device with NQA test groups configured is an NQA client, and the NQA client initiates NQA tests. An NQA server makes responses to probe packets destined to the specified destination address and port number.

Figure 39 Relationship between the NQA client and NQA server



Not all test types require the NQA server. Only the TCP, UDP echo, UDP jitter, or voice test requires both the NQA client and server, as shown in [Figure 39](#).

You can create multiple TCP or UDP listening services on the NQA server. Each listens to a specific destination address and port number. Make sure the destination IP address and port number for a listening service on the server are the same as those configured for the test group on the NQA client. Each listening service must be unique on the NQA server.

NQA probe operation procedure

An NQA probe operation involves the following steps:

1. The NQA client constructs probe packets for the specified type of NQA test, and sends them to the peer device.
2. Upon receiving the probe packets, the peer sends back responses with timestamps.
3. The NQA client computes the network performance and service quality parameters, such as the packet loss rate and round-trip time based on the received responses.

NQA configuration task list

Task	Remarks
Configuring the NQA server	Required for TCP, UDP echo, UDP jitter, and voice tests

To perform NQA tests successfully, perform the following configurations on the NQA client:

1. Enable the NQA client.
2. Create a test group and configure test parameters. The test parameters may vary with test types.
3. Configure a schedule for the NQA test group.

Complete these tasks to configure NQA client:

Task		Remarks
Enabling the NQA client		Required.
Creating an NQA test group		Required.
Configuring an NQA test group	Configuring ICMP echo tests	Required.
	Configuring DHCP tests	
	Configuring DNS tests	Use any of the approaches.

Task	Remarks
Configuring FTP tests	
Configuring HTTP tests	
Configuring UDP jitter tests	
Configuring SNMP tests	
Configuring TCP tests	
Configuring UDP echo tests	
Configuring voice tests	
Configuring DLSw tests	
Configuring the collaboration function	Optional.
Configuring threshold monitoring	Optional.
Configuring the NQA statistics collection function	Optional.
Configuring the history records saving function	Optional.
Configuring optional parameters for an NQA test group	Optional.
Configuring a schedule for an NQA test group	Required.

Configuring the NQA server

To perform TCP, UDP echo, UDP jitter, or voice tests, configure the NQA server on the peer device. The NQA server responds to the probe packets sent from the NQA client by listening to the specified destination address and port number.

To configure the NQA server:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the NQA server.	nqa server enable	Disabled by default.
3. Configure the listening service.	nqa server { tcp-connect udp-echo } ip-address port-number	The destination IP address and port number must be the same as those configured on the NQA client. A listening service must be unique on the NQA server.
4. Configure the ToS value in the packets sent by the TCP or UDP listening service.	nqa server { tcp-connect udp-echo } tos tos	Optional. By default, the ToS value is 0.

Enabling the NQA client

Configurations on the NQA client take effect only when the NQA client is enabled.

To enable the NQA client:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the NQA client.	nqa agent enable	Optional. Enabled by default.

Creating an NQA test group

Create an NQA test group before you configure NQA tests.

To create an NQA test group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an NQA test group, and enter the NQA test group view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	In the NQA test group view, you can specify the test type. You can use the nqa entry command to enter the test type view of an NQA test group with test type configured.

Configuring an NQA test group

Configuring ICMP echo tests

ICMP echo tests of an NQA test group uses ICMP echo response information to test reachability of a destination host. An ICMP echo test has the same function as the **ping** command but provides more output information. In addition, you can specify the next hop for ICMP echo tests. ICMP echo tests are used to locate connectivity problems in a network.

NQA ICMP echo tests are not supported in IPv6 networks. To test the reachability of an IPv6 address, use the **ping ipv6** command. For more information about the command, see *Network Management and Monitoring Command Reference*.

To configure ICMP echo tests:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	N/A
3. Configure the test type as ICMP echo, and enter test type view.	type icmp-echo	N/A
4. Configure the destination address of ICMP echo requests.	destination ip <i>ip-address</i>	By default, no destination IP address is configured.
5. Configure the size of the data field in each ICMP echo request.	data-size <i>size</i>	Optional. 100 bytes by default.

Step	Command	Remarks
6. Configure the string to be filled in the data field of each ICMP echo request.	data-fill <i>string</i>	Optional. By default, the string is the hexadecimal number 00010203040506070809.
7. Configure the source interface for ICMP echo requests.	source interface <i>interface-type</i> <i>interface-number</i>	Optional. By default, no source interface is configured for probe packets. The requests take the IP address of the source interface as their source IP address when no source IP address is specified. The specified source interface must be up. Otherwise, no ICMP echo requests can be sent out.
8. Configure the source IP address of ICMP echo requests.	source ip <i>ip-address</i>	Optional. By default, no source IP address is configured. If you configure both the source ip command and the source interface command, the source ip command takes effect. The source IP address must be the IP address of a local interface. The local interface must be up. Otherwise, no ICMP echo requests can be sent out.
9. Configure the next hop IP address of ICMP echo requests.	next-hop <i>ip-address</i>	Optional. By default, no next hop IP address is configured.
10. Configure optional parameters.	See " Configuring optional parameters for an NQA test group "	Optional.

Configuring DHCP tests

DHCP tests of an NQA test group are used to test if a DHCP server is on the network, and the time for the DHCP server to respond to a client request and assign an IP address to the client.

Before you start DHCP tests, configure the DHCP server. If the NQA (DHCP client) and the DHCP server are not in the same network segment, configure a DHCP relay. For the configuration of DHCP server and DHCP relay, see *Layer 3—IP Services Configuration Guide*.

The interface that performs DHCP tests does not change its IP address. A DHCP test only simulates address allocation in DHCP.

When a DHCP test completes, the NQA client sends a DHCP-RELEASE packet to release the obtained IP address.

To configuring DHCP tests:

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

Step	Command	Remarks
2. Enter NQA test group view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	N/A
3. Configure the test type as DHCP, and enter test type view.	type dhcp	N/A
4. Specify an interface to perform DHCP tests.	operation interface <i>interface-type</i> <i>interface-number</i>	By default, no interface is configured to perform DHCP tests. The specified interface must be up. Otherwise, no probe packets can be sent out.
5. Configure optional parameters.	See " Configuring optional parameters for an NQA test group "	Optional.

Configuring DNS tests

DNS tests of an NQA test group are used to test whether the NQA client can translate a domain name into an IP address through a DNS server and test the time required for resolution.

Before you start DNS tests, configure the mapping between a domain name and an IP address on a DNS server.

A DNS test simulates the domain name resolution. It does not save the mapping between the domain name and the IP address.

To configure DNS tests:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	N/A
3. Configure the test type as DNS, and enter test type view.	type dns	N/A
4. Specify the IP address of the DNS server as the destination address of DNS packets.	destination ip <i>ip-address</i>	By default, no destination IP address is configured.
5. Configure the domain name that needs to be translated.	resolve-target <i>domain-name</i>	By default, no domain name is configured.
6. Configure optional parameters.	See " Configuring optional parameters for an NQA test group "	Optional.

Configuring FTP tests

FTP tests of an NQA test group are used to test the connection between the NQA client and an FTP server and the time required for the FTP client to transfer a file to or download a file from the FTP server.

Before you start FTP tests, configure the FTP server. For example, configure a username and password that are used to log in to the FTP server. For more information about FTP server configuration, see *Fundamentals Configuration Guide*.

Follow these guidelines when you configure FTP tests:

- When you execute the **put** command, the NQA client creates a file named *file-name* of fixed size on the FTP server. The *file-name* argument does not represent any file on the NQA client. When you execute the **get** command, the client does not save the files obtained from the FTP server.
- When you get a file that does not exist on the FTP server, FTP tests fail.
- Use a small file and set a long NQA probe timeout time. A big file or short probe timeout time may result in probe timeout.

To configure FTP tests:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	N/A
3. Configure the test type as FTP, and enter test type view.	type ftp	N/A
4. Specify the IP address of the FTP server as the destination address of FTP request packets.	destination ip <i>ip-address</i>	By default, no destination IP address is configured.
5. Configure the source IP address of FTP request packets.	source ip <i>ip-address</i>	By default, no source IP address is specified. The source IP address must be the IP address of a local interface. The local interface must be up. Otherwise, no FTP requests can be sent out.
6. Configure the operation type.	operation { get put }	Optional. By default, the operation type for the FTP is get , which means obtaining files from the FTP server.
7. Configure a login username.	username <i>name</i>	By default, no login username is configured.
8. Configure a login password.	password [cipher simple] <i>password</i>	By default, no login password is configured.
9. Specify a file to be transferred between the FTP server and the FTP client.	filename <i>file-name</i>	By default, no file is specified.
10. Set the data transmission mode for FTP tests.	mode { active passive }	Optional. active by default.
11. Configure optional parameters.	See " Configuring optional parameters for an NQA test group "	Optional.

Configuring HTTP tests

HTTP tests of an NQA test group are used to test the connection between the NQA client and an HTTP server, and the time required to obtain data from the HTTP server. HTTP tests enable you to detect the connectivity and performance of the HTTP server. The TCP port must be port 80 on the HTTP server for NQA HTTP tests.

Before you start HTTP tests, configure the HTTP server.

To configure HTTP tests:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	N/A
3. Configure the test type as HTTP, and enter test type view.	type http	N/A
4. Configure the IP address of the HTTP server as the destination address of HTTP request packets.	destination ip <i>ip-address</i>	By default, no destination IP address is configured.
5. Configure the source IP address of request packets.	source ip <i>ip-address</i>	Optional. By default, no source IP address is specified. The source IP address must be the IP address of a local interface. The local interface must be up. Otherwise, no probe packets can be sent out.
6. Configure the operation type.	operation { get post }	Optional. By default, the operation type for the HTTP is get , which means obtaining data from the HTTP server.
7. Configure the website that an HTTP test visits.	url <i>url</i>	N/A
8. Configure the HTTP version used in HTTP tests.	http-version v1.0	Optional. By default, HTTP 1.0 is used.
9. Configure optional parameters.	See " Configuring optional parameters for an NQA test group "	Optional.

Configuring UDP jitter tests



IMPORTANT:

Do not perform NQA UDP jitter tests on known ports, ports from 1 to 1023. Otherwise, UDP jitter tests might fail or the corresponding services of this port might be unavailable.

Real-time services such as voice and video have high requirements on delay jitters. UDP jitter tests of an NQA test group obtain uni/bi-directional delay jitters. The test results help you verify whether a network can carry real-time services.

A UDP jitter test performs the following procedure:

1. The source sends packets to the destination port at regular intervals.
2. The destination affixes a time stamp to each packet that it receives, and then sends the packet back to the source.
3. Upon receiving the response, the source calculates the delay jitter, which reflects network performance. Delay refers to the amount of time it takes a packet to be transmitted from source to destination or from destination to source. Delay jitter is the delay variation over time.

Configuration prerequisites

UDP jitter tests require cooperation between the NQA server and the NQA client. Before you start UDP jitter tests, configure UDP listening services on the NQA server. For more information about UDP listening service configuration, see "[Configuring the NQA server](#)."

Configuration procedure

To configure UDP jitter tests:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	N/A
3. Configure the test type as UDP jitter, and enter test type view.	type udp-jitter	N/A
4. Configure the destination address of UDP packets.	destination ip <i>ip-address</i>	By default, no destination IP address is configured. The destination IP address must be the same as that of the listening service on the NQA server.
5. Configure the destination port of UDP packets.	destination port <i>port-number</i>	By default, no destination port number is configured. The destination port must be the same as that of the listening service on the NQA server.
6. Specify the source port number of UDP packets.	source port <i>port-number</i>	Optional. By default, no source port number is specified.
7. Configure the size of the data field in each UDP packet.	data-size <i>size</i>	Optional. 100 bytes by default.
8. Configure the string to be filled in the data field of each probe packet.	data-fill <i>string</i>	Optional. By default, the string is the hexadecimal number 00010203040506070809.
9. Configure the number of probe packets to be sent during each UDP jitter probe operation.	probe packet-number <i>packet-number</i>	Optional. 10 by default.

Step	Command	Remarks
10. Configure the interval for sending probe packets during each UDP jitter probe operation.	probe packet-interval <i>packet-interval</i>	Optional. 20 milliseconds by default.
11. Configure the interval the NQA client must wait for a response from the server before it regards the response is timed out.	probe packet-timeout <i>packet-timeout</i>	Optional. 3000 milliseconds by default.
12. Configure the source IP address for UDP jitter packets.	source ip <i>ip-address</i>	Optional. By default, no source IP address is specified. The source IP address must be the IP address of a local interface. The local interface must be up. Otherwise, no probe packets can be sent out.
13. Configure optional parameters.	See " Configuring optional parameters for an NQA test group "	Optional.

NOTE:

The **probe count** command specifies the number of probe operations during one UDP jitter test. The **probe packet-number** command specifies the number of probe packets sent in each UDP jitter probe operation.

Configuring SNMP tests

SNMP tests of an NQA test group are used to test the time the NQA client takes to send an SNMP packet to the SNMP agent and receive a response.

Before you start SNMP tests, enable the SNMP agent function on the device that serves as an SNMP agent. For more information about SNMP agent configuration, see "[Configuring SNMP](#)."

To configure SNMP tests:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	N/A
3. Configure the test type as SNMP, and enter test type view.	type snmp	N/A
4. Configure the destination address of SNMP packets.	destination ip <i>ip-address</i>	By default, no destination IP address is configured.
5. Specify the source port of SNMP packets.	source port <i>port-number</i>	Optional. By default, no source port number is specified.

Step	Command	Remarks
6. Configure the source IP address of SNMP packets.	source ip <i>ip-address</i>	Optional. By default, no source IP address is specified. The source IP address must be the IP address of a local interface. The local interface must be up. Otherwise, no probe packets can be sent out.
7. Configure optional parameters.	See " Configuring optional parameters for an NQA test group "	Optional.

Configuring TCP tests

TCP tests of an NQA test group are used to test the TCP connection between the NQA client and a port on the NQA server and the time for setting up a connection. The test result helps you evaluate the availability and performance of the services provided by the port on the server.

TCP tests require cooperation between the NQA server and the NQA client. Before you start TCP tests, configure a TCP listening service on the NQA server. For more information about the TCP listening service configuration, see "[Configuring the NQA server](#)."

To configure TCP tests:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name operation-tag</i>	N/A
3. Configure the test type as TCP, and enter test type view.	type tcp	N/A
4. Configure the destination address of TCP probe packets.	destination ip <i>ip-address</i>	By default, no destination IP address is configured. The destination address must be the same as the IP address of the listening service configured on the NQA server.
5. Configure the destination port of TCP probe packets.	destination port <i>port-number</i>	By default, no destination port number is configured. The destination port number must be the same as that of the listening service on the NQA server.
6. Configure the source IP address of TCP probe packets.	source ip <i>ip-address</i>	Optional. By default, no source IP address is specified. The source IP address must be the IP address of a local interface. The local interface must be up. Otherwise, no probe packets can be sent out.
7. Configure optional parameters.	See " Configuring optional parameters for an NQA test group "	Optional.

Configuring UDP echo tests

UDP echo tests of an NQA test group are used to test the connectivity and round-trip time of a UDP packet from the client to the specified UDP port on the NQA server.

UDP echo tests require cooperation between the NQA server and the NQA client. Before you start UDP echo tests, configure a UDP listening service on the NQA server. For more information about the UDP listening service configuration, see "[Configuring the NQA server](#)."

To configure UDP echo tests:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	N/A
3. Configure the test type as UDP echo, and enter test type view.	type udp-echo	N/A
4. Configure the destination address of UDP packets.	destination ip <i>ip-address</i>	By default, no destination IP address is configured. The destination address must be the same as the IP address of the listening service configured on the NQA server.
5. Configure the destination port of UDP packets.	destination port <i>port-number</i>	By default, no destination port number is configured. The destination port number must be the same as that of the listening service on the NQA server.
6. Configure the size of the data field in each UDP packet.	data-size <i>size</i>	Optional. 100 bytes by default.
7. Configure the string to be filled in the data field of each UDP packet.	data-fill <i>string</i>	Optional. By default, the string is the hexadecimal number 00010203040506070809.
8. Specify the source port of UDP packets.	source port <i>port-number</i>	Optional. By default, no source port number is specified.
9. Configure the source IP address of UDP packets.	source ip <i>ip-address</i>	Optional. By default, no source IP address is specified. The source IP address must be that of an interface on the device and the interface must be up. Otherwise, no probe packets can be sent out.
10. Configure optional parameters.	See " Configuring optional parameters for an NQA test group "	Optional.

Configuring voice tests

! IMPORTANT:

Do not perform voice tests on known ports, ports from 1 to 1023. Otherwise, the NQA test might fail or the corresponding services of these ports might be unavailable.

Voice tests of an NQA test group are used to test voice over IP (VoIP) network status, and collect VoIP network parameters so that users can adjust the network.

A voice test performs the following procedure:

1. The source (NQA client) sends voice packets of G.711 A-law, G.711 μ -law or G.729 A-law codec type at regular intervals to the destination (NQA server).
2. The destination affixes a time stamp to each voice packet that it receives and then sends it back to the source.
3. Upon receiving the packet, the source calculates results, such as the delay jitter and one-way delay based on the packet time stamps. The statistics reflect network performance.

Voice test result also includes the following parameters that reflect VoIP network performance:

- **Calculated Planning Impairment Factor (ICPIF)**—Measures impairment to voice quality in a VoIP network. It is decided by packet loss and delay. A higher value represents a lower service quality.
- **Mean Opinion Scores (MOS)**—A MOS value can be evaluated by using the ICPIF value, in the range of 1 to 5. A higher value represents a higher quality of a VoIP network.

The evaluation of voice quality depends on users' tolerance for voice quality, which should be taken into consideration. For users with higher tolerance for voice quality, use the **advantage-factor** command to configure the advantage factor. When the system calculates the ICPIF value, this advantage factor is subtracted to modify ICPIF and MOS values, so objective and subjective factors are both considered when you evaluate voice quality.

Configuration prerequisites

- Voice tests require cooperation between the NQA server and the NQA client. Before you start voice tests, configure a UDP listening service on the NQA server. For more information about UDP listening service configuration, see "[Configuring the NQA server](#)."
- Only one probe operation is performed in one voice test.

Configuration procedure

To configure voice tests:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	N/A
3. Configure the test type as voice, and enter test type view.	type voice	N/A
4. Configure the destination address of voice probe packets.	destination ip <i>ip-address</i>	By default, no destination IP address is configured for a test operation. The destination IP address must be the same as that of the listening service on the NQA server.

Step	Command	Remarks
5. Configure the destination port of voice probe packets.	destination port <i>port-number</i>	By default, no destination port number is configured. The destination port must be the same as that of the listening service on the NQA server.
6. Configure the codec type.	codec-type { g711a g711u g729a }	Optional. By default, the codec type is G.711 A-law.
7. Configure the advantage factor for calculating MOS and ICPIF values.	advantage-factor <i>factor</i>	Optional. By default, the advantage factor is 0.
8. Specify the source IP address of probe packets.	source ip <i>ip-address</i>	Optional. By default, no source IP address is specified. The source IP address must be the IP address of a local interface. The local interface must be up. Otherwise, no probe packets can be sent out.
9. Specify the source port number of probe packets.	source port <i>port-number</i>	Optional. By default, no source port number is specified.
10. Configure the size of the data field in each probe packet.	data-size <i>size</i>	Optional. By default, the probe packet size depends on the codec type. The default packet size is 172 bytes for G.711A-law and G.711 μ -law codec type, and 32 bytes for G.729 A-law codec type.
11. Configure the string to be filled in the data field of each probe packet.	data-fill <i>string</i>	Optional. By default, the string is the hexadecimal number 00010203040506070809.
12. Configure the number of probe packets to be sent during each voice probe operation.	probe packet-number <i>packet-number</i>	Optional. 1000 by default.
13. Configure the interval for sending probe packets during each voice probe operation.	probe packet-interval <i>packet-interval</i>	Optional. 20 milliseconds by default.
14. Configure the interval the NQA client must wait for a response from the server before it regards the response times out.	probe packet-timeout <i>packet-timeout</i>	Optional. 5000 milliseconds by default.
15. Configure optional parameters.	See " Configuring optional parameters for an NQA test group "	Optional.

Configuring DLSw tests

DLSw tests of an NQA test group are used to test the response time of a DLSw device.

Before you start DLSw tests, enable the DLSw function on the peer device.

To configure DLSw tests:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	N/A
3. Configure the test type as DLSw, and enter test type view.	type dlsw	N/A
4. Configure the destination address of probe packets.	destination ip <i>ip-address</i>	By default, no destination IP address is configured.
5. Configure the source IP address of probe packets.	source ip <i>ip-address</i>	Optional. By default, no source IP address is specified. The source IP address must be the IP address of a local interface. The local interface must be up. Otherwise, no probe packets can be sent out.
6. Configure optional parameters.	See " Configuring optional parameters for an NQA test group "	Optional.

Configuring the collaboration function

Collaboration is implemented by establishing reaction entries to monitor the detection results of a test group. If the number of consecutive probe failures reaches the threshold, the configured action is triggered.

To configure the collaboration function:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	N/A
3. Enter test type view of the test group.	type { dhcp dlsw dns ftp http icmp-echo snmp tcp udp-echo }	The collaboration function is not supported in UDP jitter and voice tests.
4. Configure a reaction entry.	reaction <i>item-number</i> checked-element probe-fail threshold-type consecutive <i>consecutive-occurrences</i> action-type trigger-only	Not created by default. You cannot modify the content of an existing reaction entry.
5. Exit to system view.	quit	N/A
6. Configure a track entry and associate it with the reaction entry of the NQA test group.	track <i>entry-number</i> nqa entry <i>admin-name operation-tag</i> reaction <i>item-number</i>	Not created by default.

Configuring threshold monitoring

Configuration prerequisites

Before you configure threshold monitoring, complete the following tasks:

- Configure the destination address of the trap message by using the **snmp-agent target-host** command. For more information about the **snmp-agent target-host** command, see *Network Management and Monitoring Command Reference*.
- Create an NQA test group and configure the related parameters.

Configuration guidelines

Follow these guidelines when you configure threshold monitoring:

- NQA DNS tests do not support the action of sending trap messages. The action to be triggered in DNS tests can only be the default one, **none**.
- Only the **test-complete** keyword is supported for the **reaction trap** command in a voice test.

Configuration procedure

To configure threshold monitoring:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name operation-tag</i>	N/A
3. Enter test type view of the test group.	type { dhcp dls w dns ftp http icmp-echo snmp tcp udp-echo udp-jitter voice }	N/A

Step	Command	Remarks
4. Configure threshold monitoring.	<ul style="list-style-type: none"> • Enable sending traps to the network management server under specified conditions: reaction trap { probe-failure consecutive-probe-failures test-complete test-failure cumulate-probe-failures } • Configure a reaction entry for monitoring the probe duration of a test (not supported in UDP jitter and voice tests): reaction item-number checked-element probe-duration threshold-type { accumulate accumulate-occurrences average consecutive consecutive-occurrences } threshold-value upper-threshold lower-threshold [action-type { none trap-only }] • Configure a reaction entry for monitoring the probe failure times (not supported in UDP jitter and voice tests): reaction item-number checked-element probe-fail threshold-type { accumulate accumulate-occurrences consecutive consecutive-occurrences } [action-type { none trap-only }] • Configure a reaction entry for monitoring packet round-trip time (only supported in UDP jitter and voice tests): reaction item-number checked-element rtt threshold-type { accumulate accumulate-occurrences average } threshold-value upper-threshold lower-threshold [action-type { none trap-only }] • Configure a reaction entry for monitoring the packet loss in each test (only supported in UDP jitter and voice tests): reaction item-number checked-element packet-loss threshold-type accumulate accumulate-occurrences [action-type { none trap-only }] • Configure a reaction entry for monitoring one-way delay jitter (only supported in UDP jitter and voice tests): reaction item-number checked-element { jitter-ds jitter-sd } threshold-type { accumulate accumulate-occurrences average } threshold-value upper-threshold lower-threshold [action-type { none trap-only }] • Configure a reaction entry for monitoring the one-way delay (only supported in UDP jitter and voice tests): reaction item-number checked-element { owd-ds owd-sd } threshold-value upper-threshold lower-threshold • Configure a reaction entry for monitoring the ICPIF value (only supported in voice tests): reaction item-number checked-element icpif threshold-value upper-threshold lower-threshold [action-type { none trap-only }] • Configure a reaction entry for monitoring the MOS value (only supported in voice tests): reaction item-number checked-element mos threshold-value upper-threshold lower-threshold [action-type { none trap-only }] 	<p>Configure to send traps.</p> <p>No traps are sent to the network management server by default.</p>

Configuring the NQA statistics collection function

NQA groups tests completed in a time period for a test group, and calculates the test result statistics. The statistics form a statistics group. To view information about the statistics groups, use the **display nqa statistics** command. To set the interval for collecting statistics, use the **statistics interval** command.

When the number of statistics groups kept reaches the upper limit and a new statistics group is to be saved, the oldest statistics group is deleted. To set the maximum number of statistics groups that can be kept, use the **statistics max-group** command.

A statistics group is formed after the last test is completed within the specified interval. Statistics groups have an aging mechanism. A statistics group is deleted when its hold time expires. To set the hold time of statistics groups for a test group, use the **statistics hold-time** command.

Follow these guidelines when you configure the NQA statistics collection function:

- The NQA statistics collection function is not supported in DHCP tests.
- If you use the **frequency** command to set the frequency between two consecutive tests to 0, only one test is performed, and no statistics group information is collected.

To configure the NQA statistics collection function:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name operation-tag</i>	N/A
3. Enter test type view of the test group.	type { <i>dls</i> <i>dns</i> <i>ftp</i> <i>http</i> <i>icmp-echo</i> <i>snmp</i> <i>tcp</i> <i>udp-echo</i> <i>udp-jitter</i> <i>voice</i> }	N/A
4. Configure the interval for collecting the statistics of test results.	statistics interval <i>interval</i>	Optional. 60 minutes by default.
5. Configure the maximum number of statistics groups that can be kept.	statistics max-group <i>number</i>	Optional. 2 by default. To disable collecting NQA statistics, set the maximum number to 0.
6. Configure the hold time of statistics groups.	statistics hold-time <i>hold-time</i>	Optional. 120 minutes by default.

Configuring the history records saving function

The history records saving function enables the system to save the history records of NQA tests. To view the history records of a test group, use the **display nqa history** command.

The configuration task also allows you to configure the following elements:

- **Lifetime of the history records**—The records are removed when the lifetime is reached.
- **The maximum number of history records that can be saved in a test group**—If the number of history records in a test group exceeds the maximum number, the earliest history records are removed.

To configure the history records saving function of an NQA test group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	N/A
3. Enter NQA test type view.	type { dhcp dls w dns ftp http icmp-echo snmp tcp udp-echo udp-jitter voice }	N/A
4. Enable the saving of the history records of the NQA test group.	history-record enable	By default, history records of the NQA test group are not saved.
5. Set the lifetime of the history records in an NQA test group.	history-record keep-time <i>keep-time</i>	Optional. By default, the history records in the NQA test group are kept for 120 minutes.
6. Configure the maximum number of history records that can be saved for a test group.	history-record number <i>number</i>	Optional. By default, the maximum number of records that can be saved for a test group is 50.

Configuring optional parameters for an NQA test group

Optional parameters for an NQA test group are valid only for tests in this test group.

Unless otherwise specified, the following optional parameters are applicable to all test types.

To configure optional parameters for an NQA test group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter NQA test group view.	nqa entry <i>admin-name</i> <i>operation-tag</i>	N/A
3. Enter test type view of a test group.	type { dhcp dls w dns ftp http icmp-echo snmp tcp udp-echo udp-jitter voice }	N/A
4. Configure the description for a test group.	description <i>text</i>	Optional. By default, no description is available for a test group.

Step	Command	Remarks
5. Configure the interval between two consecutive tests for a test group.	frequency <i>interval</i>	Optional. By default, the interval between two consecutive tests for a test group is 0 milliseconds. Only one test is performed. If the last test is not completed when the interval specified by the frequency command is reached, a new test does not start.
6. Configure the number of probe operations to be performed in one test.	probe count <i>times</i>	Optional. By default, one probe operation is performed in one test. Not available for voice tests, Only one probe operation can be performed in one voice test.
7. Configure the NQA probe timeout time.	probe timeout <i>timeout</i>	Optional. By default, the timeout time is 3000 milliseconds. Not available for UDP jitter tests.
8. Configure the maximum number of hops a probe packet traverses in the network.	ttl <i>value</i>	Optional. 20 by default. Not available for DHCP tests.
9. Configure the ToS field in an IP packet header in an NQA probe packet.	tos <i>value</i>	Optional. 0 by default.
10. Enable the routing table bypass function.	route-option bypass-route	Optional. Disabled by default. Not available for DHCP tests.

Configuring a schedule for an NQA test group

You can configure a schedule for an NQA test group by setting the start time and test duration for a test group.

A test group performs tests between the scheduled start time and the end time (the start time plus test duration). If the scheduled start time is ahead of the system time, the test group starts testing immediately. If both the scheduled start and end time are behind the system time, no test will start. To view the current system time, use the **display clock** command.

Configuration prerequisites

Before you configure a schedule for an NQA test group, complete the following tasks:

- Configure test parameters required for the test type.
- Configure the NQA server for tests that require cooperation with the NQA server.

Configuration guidelines

Follow these guidelines when you schedule an NQA test group:

- After an NQA test group is scheduled, you cannot enter the test group view or test type view.
- System adjustment does not affect started or completed test groups. It only affects test groups that have not started.

Configuration procedure

To schedule an NQA test group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure a schedule for an NQA test group.	nqa schedule <i>admin-name operation-tag start-time</i> { <i>hh:mm:ss</i> [<i>yyyy/mm/dd</i>] now } lifetime { <i>lifetime</i> forever }	now specifies the test group starts testing immediately. forever specifies that the tests do not stop unless you use the undo nqa schedule command.
3. Configure the maximum number of tests that the NQA client can simultaneously perform.	nqa agent max-concurrent <i>number</i>	Optional. By default, the maximum number of tests that the NQA client can simultaneously perform is 2.

Displaying and maintaining NQA

Task	Command	Remarks
Display history records of NQA test groups.	display nqa history [<i>admin-name operation-tag</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the current monitoring results of reaction entries.	display nqa reaction counters [<i>admin-name operation-tag</i> [<i>item-number</i>]] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the results of the last NQA test.	display nqa result [<i>admin-name operation-tag</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display statistics of test results for the specified or all test groups.	display nqa statistics [<i>admin-name operation-tag</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display NQA server status.	display nqa server status [{ begin exclude include } <i>regular-expression</i>]	Available in any view

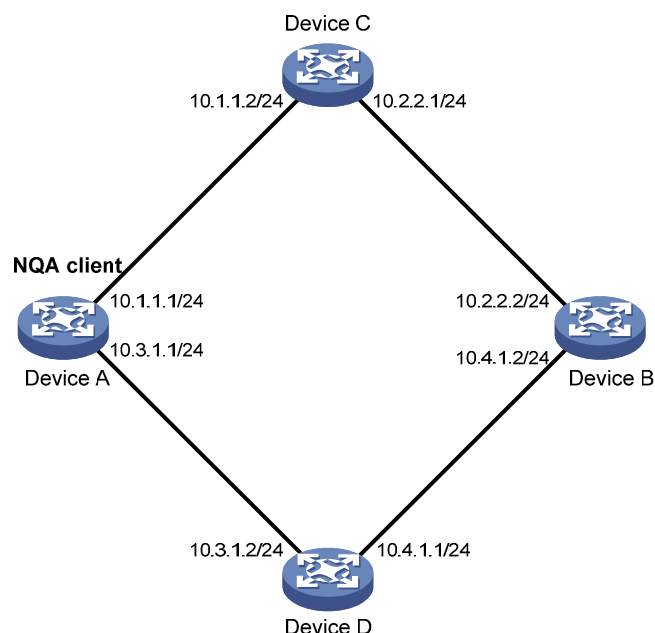
NQA configuration examples

ICMP echo test configuration example

Network requirements

As shown in [Figure 40](#), configure NQA ICMP echo tests to test whether the NQA client (Device A) can send packets through a specific next hop to the specified destination (Device B) and test the round-trip time of the packets.

Figure 40 Network diagram



Configuration procedure

Before you make the configuration, make sure the devices can reach each other.

Create an ICMP echo test group, and specify 10.2.2.2 as the destination IP address for ICMP echo requests to be sent.

```
<DeviceA> system-view
[DeviceA] nga entry admin test
[DeviceA-nga-admin-test] type icmp-echo
[DeviceA-nga-admin-test-icmp-echo] destination ip 10.2.2.2
```

Configure 10.1.1.2 as the next hop IP address for ICMP echo requests. The ICMP echo requests are sent to Device C to Device B (the destination).

```
[DeviceA-nga-admin-test-icmp-echo] next-hop 10.1.1.2
```

Configure the device to perform 10 probe operations per test, perform tests at an interval of 5000 milliseconds. Set the NQA probe timeout time as 500 milliseconds.

```
[DeviceA-nga-admin-test-icmp-echo] probe count 10
[DeviceA-nga-admin-test-icmp-echo] probe timeout 500
[DeviceA-nga-admin-test-icmp-echo] frequency 5000
```

Enable the saving of history records and configure the maximum number of history records that can be saved for a test group.

```
[DeviceA-nqa-admin-test-icmp-echo] history-record enable
[DeviceA-nqa-admin-test-icmp-echo] history-record number 10
[DeviceA-nqa-admin-test-icmp-echo] quit
```

Start ICMP echo tests.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

Stop the ICMP echo tests after a period of time.

```
[DeviceA] undo nqa schedule admin test
```

Display the results of the last ICMP echo test.

```
[DeviceA] display nqa result admin test

NQA entry (admin admin, tag test) test results:
  Destination IP address: 10.2.2.2
    Send operation times: 10          Receive response times: 10
    Min/Max/Average round trip time: 2/5/3
    Square-Sum of round trip time: 96
    Last succeeded probe time: 2011-01-23 15:00:01.2
  Extended results:
    Packet loss in test: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to sequence error: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packet(s) arrived late: 0
```

Display the history of ICMP echo tests.

```
[DeviceA] display nqa history admin test

NQA entry (admin admin, tag test) history record(s):
```

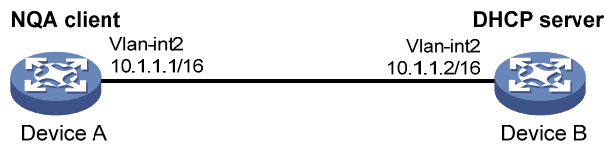
Index	Response	Status	Time
370	3	Succeeded	2011-01-23 15:00:01.2
369	3	Succeeded	2011-01-23 15:00:01.2
368	3	Succeeded	2011-01-23 15:00:01.2
367	5	Succeeded	2011-01-23 15:00:01.2
366	3	Succeeded	2011-01-23 15:00:01.2
365	3	Succeeded	2011-01-23 15:00:01.2
364	3	Succeeded	2011-01-23 15:00:01.1
363	2	Succeeded	2011-01-23 15:00:01.1
362	3	Succeeded	2011-01-23 15:00:01.1
361	2	Succeeded	2011-01-23 15:00:01.1

DHCP test configuration example

Network requirements

As shown in [Figure 41](#), configure NQA DHCP tests to test the time required for Device A to obtain an IP address from the DHCP server (Device B).

Figure 41 Network diagram



Configuration procedure

Create a DHCP test group, and specify interface VLAN-interface 2 to perform NQA DHCP tests.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type dhcp
[DeviceA-nqa-admin-test-dhcp] operation interface vlan-interface 2
```

Enable the saving of history records.

```
[DeviceA-nqa-admin-test-dhcp] history-record enable
[DeviceA-nqa-admin-test-dhcp] quit
```

Start DHCP tests.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

Stop DHCP tests after a period of time.

```
[DeviceA] undo nqa schedule admin test
```

Display the result of the last DHCP test.

```
[DeviceA] display nqa result admin test

NQA entry (admin admin, tag test) test results:
  Send operation times: 1          Receive response times: 1
  Min/Max/Average round trip time: 624/624/624
  Square-Sum of round trip time: 389376
  Last succeeded probe time: 2011-01-22 09:56:03.2

Extended results:
  Packet loss in test: 0%
  Failures due to timeout: 0
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to sequence error: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packet(s) arrived late: 0
```

Display the history of DHCP tests.

```
[DeviceA] display nqa history admin test

NQA entry (admin admin, tag test) history record(s):
```

Index	Response	Status	Time
1	624	Succeeded	2011-01-22 09:56:03.2

DNS test configuration example

Network requirements

As shown in Figure 42, configure NQA DNS tests to test whether Device A can translate the domain name **host.com** into an IP address through the DNS server and test the time required for resolution.

Figure 42 Network diagram



Configuration procedure

Before you make the configuration, make sure the devices can reach each other.

Create a DNS test group.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type dns
```

Specify the IP address of the DNS server 10.2.2.2 as the destination address for DNS tests, and specify the domain name that needs to be translated as **host.com**.

```
[DeviceA-nqa-admin-test-dns] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-dns] resolve-target host.com
```

Enable the saving of history records.

```
[DeviceA-nqa-admin-test-dns] history-record enable
[DeviceA-nqa-admin-test-dns] quit
```

Start DNS tests.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

Stop the DNS tests after a period of time.

```
[DeviceA] undo nqa schedule admin test
```

Display the results of the last DNS test.

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
  Destination IP address: 10.2.2.2
  Send operation times: 1                Receive response times: 1
  Min/Max/Average round trip time: 62/62/62
  Square-Sum of round trip time: 3844
  Last succeeded probe time: 2011-01-10 10:49:37.3
Extended results:
  Packet loss in test: 0%
  Failures due to timeout: 0
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to sequence error: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
```

```
Packet(s) arrived late: 0
```

```
# Display the history of DNS tests.
```

```
[DeviceA] display nqa history admin test
```

```
NQA entry (admin admin, tag test) history record(s):
```

Index	Response	Status	Time
1	62	Succeeded	2011-01-10 10:49:37.3

FTP test configuration example

Network requirements

As shown in [Figure 43](#), configure NQA FTP tests to test the connection with a specific FTP server and the time required for Device A to upload a file to the FTP server. The login username is **admin**, the login password is **systemtest**, and the file to be transferred to the FTP server is **config.txt**.

Figure 43 Network diagram



Configuration procedure

Before you make the configuration, make sure the devices can reach each other.

```
# Create an FTP test group.
```

```
<DeviceA> system-view
```

```
[DeviceA] nqa entry admin test
```

```
[DeviceA-nqa-admin-test] type ftp
```

```
# Specify the IP address of the FTP server 10.2.2.2 as the destination IP address for FTP tests.
```

```
[DeviceA-nqa-admin-test-ftp] destination ip 10.2.2.2
```

```
# Specify 10.1.1.1 as the source IP address for probe packets.
```

```
[DeviceA-nqa-admin-test-ftp] source ip 10.1.1.1
```

```
# Set the FTP username to admin, and password to systemtest.
```

```
[DeviceA-nqa-admin-test-ftp] username admin
```

```
[DeviceA-nqa-admin-test-ftp] password systemtest
```

```
# Configure the device to upload file config.txt to the FTP server for each probe operation.
```

```
[DeviceA-nqa-admin-test-ftp] operation put
```

```
[DeviceA-nqa-admin-test-ftp] filename config.txt
```

```
# Enable the saving of history records.
```

```
[DeviceA-nqa-admin-test-ftp] history-record enable
```

```
[DeviceA-nqa-admin-test-ftp] quit
```

```
# Start FTP tests.
```

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

```
# Stop the FTP tests after a period of time.
```

```
[DeviceA] undo nqa schedule admin test
```

```
# Display the results of the last FTP test.
```

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
  Destination IP address: 10.2.2.2
    Send operation times: 1          Receive response times: 1
    Min/Max/Average round trip time: 173/173/173
    Square-Sum of round trip time: 29929
    Last succeeded probe time: 2011-01-22 10:07:28.6
Extended results:
  Packet loss in test: 0%
  Failures due to timeout: 0
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to sequence error: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packet(s) arrived late: 0
```

Display the history of FTP tests.

```
[DeviceA] display nqa history admin test
NQA entry (admin admin, tag test) history record(s):
  Index      Response      Status      Time
  1          173           Succeeded   2011-01-22 10:07:28.6
```

HTTP test configuration example

Network requirements

As shown in [Figure 44](#), configure NQA HTTP tests to test the connection with a specific HTTP server and the time required to obtain data from the HTTP server.

Figure 44 Network diagram



Configuration procedure

Before you make the configuration, make sure the devices can reach each other.

Create an HTTP test group.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type http
```

Specify the IP address of the HTTP server 10.2.2.2 as the destination IP address for HTTP tests.

```
[DeviceA-nqa-admin-test-http] destination ip 10.2.2.2
```

Configure the device to get data from the HTTP server for each HTTP probe operation. (get is the default HTTP operation type, and this step is optional.)

```
[DeviceA-nqa-admin-test-http] operation get
```

Configure HTTP tests to visit website **/index.htm**.

```
[DeviceA-nqa-admin-test-http] url /index.htm

# Configure the HTTP version 1.0 to be used in HTTP tests. (Version 1.0 is the default version, and this step
is optional.)
[DeviceA-nqa-admin-test-http] http-version v1.0

# Enable the saving of history records.
[DeviceA-nqa-admin-test-http] history-record enable
[DeviceA-nqa-admin-test-http] quit

# Start HTTP tests.
[DeviceA] nqa schedule admin test start-time now lifetime forever

# Stop HTTP tests after a period of time.
[DeviceA] undo nqa schedule admin test

# Display results of the last HTTP test.
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
  Destination IP address: 10.2.2.2
    Send operation times: 1                Receive response times: 1
  Min/Max/Average round trip time: 64/64/64
  Square-Sum of round trip time: 4096
  Last succeeded probe time: 2011-01-22 10:12:47.9
Extended results:
  Packet loss in test: 0%
  Failures due to timeout: 0
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to sequence error: 0
  Failures due to internal error: 0
  Failures due to other errors:
  Packet(s) arrived late: 0

# Display the history of HTTP tests.
[DeviceA] display nqa history admin test
NQA entry (admin admin, tag test) history record(s):
  Index      Response      Status      Time
  1          64           Succeeded   2011-01-22 10:12:47.9
```

UDP jitter test configuration example

Network requirements

As shown in [Figure 45](#), configure NQA UDP jitter tests to test the delay jitter of packet transmission between Device A and Device B.

Figure 45 Network diagram



Configuration procedure

Before you make the configuration, make sure the devices can reach each other.

1. Enable the NQA server, and configure a listening service to listen to IP address 10.2.2.2 and UDP port 9000 on Device B.

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

2. Configure Device A:

Create a UDP jitter test group.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type udp-jitter
```

Configure UDP jitter packets to use 10.2.2.2 as the destination IP address and port 9000 as the destination port.

```
[DeviceA-nqa-admin-test-udp-jitter] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-udp-jitter] destination port 9000
```

Configure the device to perform UDP jitter tests at an interval of 1000 milliseconds.

```
[DeviceA-nqa-admin-test-udp-jitter] frequency 1000
[DeviceA-nqa-admin-test-udp-jitter] quit
```

Start UDP jitter tests.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

Stop UDP jitter tests after a period of time.

```
[DeviceA] undo nqa schedule admin test
```

Display the result of the last UDP jitter test.

```
[DeviceA] display nqa result admin test
```

NQA entry (admin admin, tag test) test results:

Destination IP address: 10.2.2.2

Send operation times: 10

Receive response times: 10

Min/Max/Average round trip time: 15/32/17

Square-Sum of round trip time: 3235

Last succeeded probe time: 2011-01-29 13:56:17.6

Extended results:

Packet loss in test: 0%

Failures due to timeout: 0

Failures due to disconnect: 0

Failures due to no connection: 0

Failures due to sequence error: 0

Failures due to internal error: 0

Failures due to other errors: 0

Packet(s) arrived late: 0

UDP-jitter results:

RTT number: 10

Min positive SD: 4

Min positive DS: 1

Max positive SD: 21

Max positive DS: 28

Positive SD number: 5

Positive DS number: 4

Positive SD sum: 52

Positive DS sum: 38

Positive SD average: 10	Positive DS average: 10
Positive SD square sum: 754	Positive DS square sum: 460
Min negative SD: 1	Min negative DS: 6
Max negative SD: 13	Max negative DS: 22
Negative SD number: 4	Negative DS number: 5
Negative SD sum: 38	Negative DS sum: 52
Negative SD average: 10	Negative DS average: 10
Negative SD square sum: 460	Negative DS square sum: 754
One way results:	
Max SD delay: 15	Max DS delay: 16
Min SD delay: 7	Min DS delay: 7
Number of SD delay: 10	Number of DS delay: 10
Sum of SD delay: 78	Sum of DS delay: 85
Square sum of SD delay: 666	Square sum of DS delay: 787
SD lost packet(s): 0	DS lost packet(s): 0
Lost packet(s) for unknown reason: 0	

Display the statistics of UDP jitter tests.

[DeviceA] display nqa statistics admin test

NQA entry (admin admin, tag test) test statistics:

NO. : 1

Destination IP address: 10.2.2.2

Start time: 2011-01-29 13:56:14.0

Life time: 47 seconds

Send operation times: 410 Receive response times: 410

Min/Max/Average round trip time: 1/93/19

Square-Sum of round trip time: 206176

Extended results:

Packet loss in test: 0%

Failures due to timeout: 0

Failures due to disconnect: 0

Failures due to no connection: 0

Failures due to sequence error: 0

Failures due to internal error: 0

Failures due to other errors: 0

Packet(s) arrived late: 0

UDP-jitter results:

RTT number: 410	
Min positive SD: 3	Min positive DS: 1
Max positive SD: 30	Max positive DS: 79
Positive SD number: 186	Positive DS number: 158
Positive SD sum: 2602	Positive DS sum: 1928
Positive SD average: 13	Positive DS average: 12
Positive SD square sum: 45304	Positive DS square sum: 31682
Min negative SD: 1	Min negative DS: 1
Max negative SD: 30	Max negative DS: 78
Negative SD number: 181	Negative DS number: 209
Negative SD sum: 181	Negative DS sum: 209
Negative SD average: 13	Negative DS average: 14

Negative SD square sum: 46994	Negative DS square sum: 3030
One way results:	
Max SD delay: 46	Max DS delay: 46
Min SD delay: 7	Min DS delay: 7
Number of SD delay: 410	Number of DS delay: 410
Sum of SD delay: 3705	Sum of DS delay: 3891
Square sum of SD delay: 45987	Square sum of DS delay: 49393
SD lost packet(s): 0	DS lost packet(s): 0
Lost packet(s) for unknown reason: 0	

NOTE:

The **display nqa history** command does not show the results of UDP jitter tests. To know the result of a UDP jitter test, use the **display nqa result** command to view the probe results of the latest NQA test, or use the **display nqa statistics** command to view the statistics of NQA tests.

SNMP test configuration example

Network requirements

As shown in Figure 46, configure NQA SNMP tests to test the time it takes for Device A to send an SNMP query packet to the SNMP agent and receive a response packet.

Figure 46 Network diagram



Configuration procedure

Before you make the configuration, make sure the devices can reach each other.

1. Enable the SNMP agent service and set the SNMP version to **all**, the read community to **public**, and the write community to **private on Device B**.

```

<DeviceB> system-view
[DeviceB] snmp-agent
[DeviceB] snmp-agent sys-info version all
[DeviceB] snmp-agent community read public
[DeviceB] snmp-agent community write private
  
```

2. Configure Device A:

Create an SNMP test group, and configure SNMP packets to use 10.2.2.2 as their destination IP address.

```

<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type snmp
[DeviceA-nqa-admin-test-snmp] destination ip 10.2.2.2
  
```

Enable the saving of history records.

```

[DeviceA-nqa-admin-test-snmp] history-record enable
[DeviceA-nqa-admin-test-snmp] quit
  
```



```
# Start SNMP tests.
[DeviceA] nqa schedule admin test start-time now lifetime forever

# Stop the SNMP tests after a period of time.
[DeviceA] undo nqa schedule admin test

# Display the results of the last SNMP test.
[DeviceA] display nqa result admin test

NQA entry (admin admin, tag test) test results:
  Destination IP address: 10.2.2.2
    Send operation times: 1                Receive response times: 1
  Min/Max/Average round trip time: 50/50/50
  Square-Sum of round trip time: 2500
  Last succeeded probe time: 2011-01-22 10:24:41.1
Extended results:
  Packet loss in test: 0%
  Failures due to timeout: 0
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to sequence error: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packet(s) arrived late: 0

# Display the history of SNMP tests.
[DeviceA] display nqa history admin test

NQA entry (admin admin, tag test) history record(s):
  Index      Response      Status      Time
  1          50           Timeout     2011-01-22 10:24:41.1
```

TCP test configuration example

Network requirements

As shown in [Figure 47](#), configure NQA TCP tests to test the time for establishing a TCP connection between Device A and Device B.

Figure 47 Network diagram



Configuration procedure

Before you make the configuration, make sure the devices can reach each other.

1. Enable the NQA server, and configure a listening service to listen to IP address 10.2.2.2 and TCP port 9000 on Device B.

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server tcp-connect 10.2.2.2 9000
```

2. Configure Device A:

```

# Create a TCP test group.
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type tcp

# Configure TCP probe packets to use 10.2.2.2 as the destination IP address and port 9000 as
the destination port.
[DeviceA-nqa-admin-test-tcp] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-tcp] destination port 9000

# Enable the saving of history records.
[DeviceA-nqa-admin-test-tcp] history-record enable
[DeviceA-nqa-admin-test-tcp] quit

# Start TCP tests.
[DeviceA] nqa schedule admin test start-time now lifetime forever

# Stop the TCP tests after a period of time.
[DeviceA] undo nqa schedule admin test

# Display the results of the last TCP test.
[DeviceA] display nqa result admin test
  NQA entry (admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1                      Receive response times: 1
      Min/Max/Average round trip time: 13/13/13
      Square-Sum of round trip time: 169
      Last succeeded probe time: 2011-01-22 10:27:25.1
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0

# Display the history of TCP tests.
[DeviceA] display nqa history admin test
  NQA entry (admin admin, tag test) history record(s):

```

Index	Response	Status	Time
1	13	Succeeded	2011-01-22 10:27:25.1

UDP echo test configuration example

Network requirements

As shown in [Figure 48](#), configure NQA UDP echo tests to test the round-trip time between Device A and Device B. The destination port number is 8000.

Figure 48 Network diagram



Configuration procedure

Before you make the configuration, make sure the devices can reach each other.

1. Enable the NQA server, and configure a listening service to listen to IP address 10.2.2.2 and UDP port 8000 on Device B.

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 8000
```

2. Configure Device A:

Create a UDP echo test group.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type udp-echo
```

Configure UDP packets to use 10.2.2.2 as the destination IP address and port 8000 as the destination port.

```
[DeviceA-nqa-admin-test-udp-echo] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-udp-echo] destination port 8000
```

Enable the saving of history records.

```
[DeviceA-nqa-admin-test-udp-echo] history-record enable
[DeviceA-nqa-admin-test-udp-echo] quit
```

Start UDP echo tests.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

Stop UDP echo tests after a period of time.

```
[DeviceA] undo nqa schedule admin test
```

Display the results of the last UDP echo test.

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
  Destination IP address: 10.2.2.2
    Send operation times: 1          Receive response times: 1
  Min/Max/Average round trip time: 25/25/25
  Square-Sum of round trip time: 625
  Last succeeded probe time: 2011-01-22 10:36:17.9
Extended results:
  Packet loss in test: 0%
  Failures due to timeout: 0
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to sequence error: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packet(s) arrived late: 0
```

```
# Display the history of UDP echo tests.
[DeviceA] display nqa history admin test
NQA entry (admin admin, tag test) history record(s):
  Index      Response      Status      Time
  1          25          Succeeded   2011-01-22 10:36:17.9
```

Voice test configuration example

Network requirements

As shown in [Figure 49](#), configure NQA voice tests to test the delay jitter of voice packet transmission and voice quality between Device A and Device B.

Figure 49 Network diagram



Configuration procedure

Before you make the configuration, make sure the devices can reach each other.

1. Enable the NQA server, and configure a listening service to listen to IP address 10.2.2.2 and UDP port 9000 on Device B.

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

2. Configure Device A:

Create a voice test group.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type voice
```

Configure voice probe packets to use 10.2.2.2 as the destination IP address and port 9000 as the destination port.

```
[DeviceA-nqa-admin-test-voice] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-voice] destination port 9000
[DeviceA-nqa-admin-test-voice] quit
```

Start voice tests.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

Stop the voice tests after a period of time.

```
[DeviceA] undo nqa schedule admin test
```

Display the result of the last voice test.

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
  Destination IP address: 10.2.2.2
    Send operation times: 1000          Receive response times: 1000
  Min/Max/Average round trip time: 31/1328/33
  Square-Sum of round trip time: 2844813
```

```

    Last succeeded probe time: 2011-01-13 09:49:31.1
Extended results:
    Packet loss in test: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to sequence error: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packet(s) arrived late: 0
Voice results:
    RTT number: 1000
    Min positive SD: 1
    Max positive SD: 204
    Positive SD number: 257
    Positive SD sum: 759
    Positive SD average: 2
    Positive SD square sum: 54127
    Min negative SD: 1
    Max negative SD: 203
    Negative SD number: 255
    Negative SD sum: 759
    Negative SD average: 2
    Negative SD square sum: 53655
    Min positive DS: 1
    Max positive DS: 1297
    Positive DS number: 259
    Positive DS sum: 1797
    Positive DS average: 6
    Positive DS square sum: 1691967
    Min negative DS: 1
    Max negative DS: 1297
    Negative DS number: 259
    Negative DS sum: 1796
    Negative DS average: 6
    Negative DS square sum: 1691776
One way results:
    Max SD delay: 343
    Min SD delay: 343
    Number of SD delay: 1
    Sum of SD delay: 343
    Square sum of SD delay: 117649
    SD lost packet(s): 0
    Lost packet(s) for unknown reason: 0
    Max DS delay: 985
    Min DS delay: 985
    Number of DS delay: 1
    Sum of DS delay: 985
    Square sum of DS delay: 970225
    DS lost packet(s): 0
Voice scores:
    MOS value: 4.38
    ICPIF value: 0

```

Display the statistics of voice tests.

```

[DeviceA] display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
NO. : 1
Destination IP address: 10.2.2.2
    Start time: 2011-01-13 09:45:37.8
    Life time: 331 seconds
    Send operation times: 4000
    Receive response times: 4000
    Min/Max/Average round trip time: 15/1328/32
    Square-Sum of round trip time: 7160528
Extended results:
    Packet loss in test: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0

```

```

Failures due to no connection: 0
Failures due to sequence error: 0
Failures due to internal error: 0
Failures due to other errors: 0
Packet(s) arrived late: 0
Voice results:
RTT number: 4000
Min positive SD: 1
Max positive SD: 360
Positive SD number: 1030
Positive SD sum: 4363
Positive SD average: 4
Positive SD square sum: 497725
Min negative SD: 1
Max negative SD: 360
Negative SD number: 1028
Negative SD sum: 1028
Negative SD average: 4
Negative SD square sum: 495901
Min positive DS: 1
Max positive DS: 1297
Positive DS number: 1024
Positive DS sum: 5423
Positive DS average: 5
Positive DS square sum: 2254957
Min negative DS: 1
Max negative DS: 1297
Negative DS number: 1022
Negative DS sum: 1022
Negative DS average: 5
Negative DS square sum: 5419
One way results:
Max SD delay: 359
Min SD delay: 0
Number of SD delay: 4
Sum of SD delay: 1390
Square sum of SD delay: 483202
SD lost packet(s): 0
Lost packet(s) for unknown reason: 0
Max DS delay: 985
Min DS delay: 0
Number of DS delay: 4
Sum of DS delay: 1079
Square sum of DS delay: 973651
DS lost packet(s): 0
Voice scores:
Max MOS value: 4.38
Max ICPIF value: 0
Min MOS value: 4.38
Min ICPIF value: 0

```

NOTE:

The **display nqa history** command cannot show you the results of voice tests. To know the result of a voice test, use the **display nqa result** command to view the probe results of the latest NQA test, or use the **display nqa statistics** command to view the statistics of NQA tests.

DLSw test configuration example

Network requirements

As shown in [Figure 50](#), configure NQA DLSw tests to test the response time of the DLSw device.

Figure 50 Network diagram



Configuration procedure

Before you make the configuration, make sure the devices can reach each other.

Create a DLSw test group, and configure DLSw probe packets to use 10.2.2.2 as the destination IP address.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type dlsw
[DeviceA-nqa-admin-test-dlsw] destination ip 10.2.2.2
```

Enable the saving of history records.

```
[DeviceA-nqa-admin-test-dlsw] history-record enable
[DeviceA-nqa-admin-test-dlsw] quit
```

Start DLSw tests.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

Stop the DLSw tests after a period of time.

```
[DeviceA] undo nqa schedule admin test
```

Display the result of the last DLSw test.

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
  Destination IP address: 10.2.2.2
    Send operation times: 1          Receive response times: 1
    Min/Max/Average round trip time: 19/19/19
    Square-Sum of round trip time: 361
    Last succeeded probe time: 2011-01-22 10:40:27.7
Extended results:
  Packet loss in test: 0%
  Failures due to timeout: 0
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to sequence error: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packet(s) arrived late: 0
```

Display the history of DLSw tests.

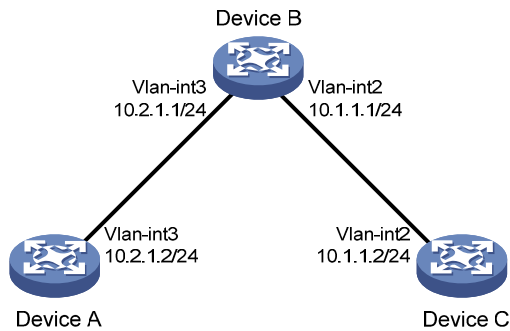
```
[DeviceA] display nqa history admin test
NQA entry (admin admin, tag test) history record(s):
  Index      Response      Status      Time
  1          19           Succeeded   2011-01-22 10:40:27.7
```

NQA collaboration configuration example

Network requirements

As shown in [Figure 51](#), configure a static route to Device C on Device A, with Device B as the next hop. Associate the static route, track entry, and NQA test group to verify whether static route is active in real time.

Figure 51 Network diagram



Configuration procedure

1. Assign each interface an IP address. (Details not shown.)
2. Configure a static route, whose destination address is 10.2.1.1, and associate the static route with track entry 1 on Device A.

```
<DeviceA> system-view
[DeviceA] ip route-static 10.1.1.2 24 10.2.1.1 track 1
```

3. On Device A, create an NQA test group:

Create an NQA test group with the administrator name being **admin** and operation tag being **test**.

```
[DeviceA] nqa entry admin test
```

Configure the test type of the NQA test group as ICMP echo.

```
[DeviceA-nqa-admin-test] type icmp-echo
```

Configure ICMP echo requests to use 10.2.1.1 as their destination IP address.

```
[DeviceA-nqa-admin-test-icmp-echo] destination ip 10.2.1.1
```

Configure the device to perform tests at an interval of 100 milliseconds.

```
[DeviceA-nqa-admin-test-icmp-echo] frequency 100
```

Create reaction entry 1. If the number of consecutive probe failures reaches 5, collaboration with other modules is triggered.

```
[DeviceA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail
threshold-type consecutive 5 action-type trigger-only
```

```
[DeviceA-nqa-admin-test-icmp-echo] quit
```

Configure the test start time and test duration for the test group.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

4. Create track entry 1 on Device A, and associate it with reaction entry 1 of the NQA test group (admin-test).

```
[DeviceA] track 1 nqa entry admin test reaction 1
```

Verifying the configuration

On Device A, display information about all track entries.

```
[DeviceA] display track all
```

Track ID: 1

Status: Positive

Notification delay: Positive 0, Negative 0 (in seconds)

Reference object:

NQA entry: admin test

Reaction: 1

Display brief information about active routes in the routing table on Device A.

```
[DeviceA] display ip routing-table
```

Routing Tables: Public

Destinations : 5 Routes : 5

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	Static	60	0	10.2.1.1	Vlan3
10.2.1.0/24	Direct	0	0	10.2.1.2	Vlan3
10.2.1.2/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

The output shows that the static route with the next hop 10.2.1.1 is active, and the status of the track entry is positive. The static route configuration works.

Remove the IP address of VLAN-interface 3 on Device B.

```
<DeviceB> system-view
```

```
[DeviceB] interface vlan-interface 3
```

```
[DeviceB-Vlan-interface3] undo ip address
```

On Device A, display information about all track entries.

```
[DeviceA] display track all
```

Track ID: 1

Status: Negative

Notification delay: Positive 0, Negative 0 (in seconds)

Reference object:

NQA entry: admin test

Reaction: 1

Display brief information about active routes in the routing table on Device A.

```
[DeviceA] display ip routing-table
```

Routing Tables: Public

Destinations : 4 Routes : 4

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.2.1.0/24	Direct	0	0	10.2.1.2	Vlan3
10.2.1.2/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

The output shows that the next hop 10.2.1.1 of the static route is not reachable, and the status of the track entry is negative. The static route does not work.

Configuring sFlow

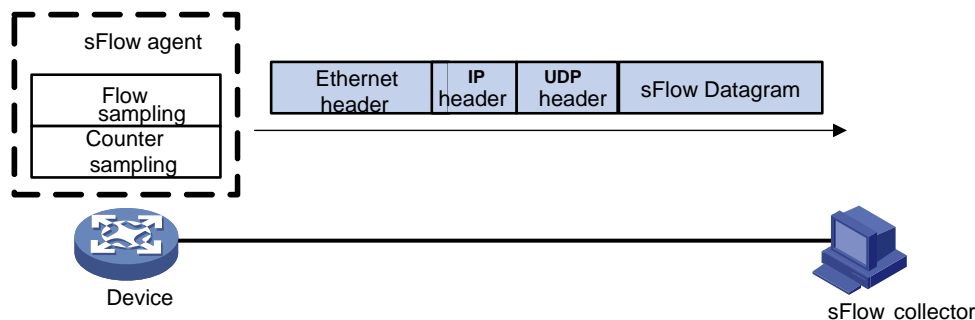
Sampled Flow (sFlow) is a traffic monitoring technology used to collect and analyze traffic statistics.

As shown in [Figure 52](#), the sFlow system involves an sFlow agent embedded in a device and a remote sFlow collector. The sFlow agent collects interface counter information and packet information and encapsulates the sampled information into sFlow packets. When the sFlow packet buffer is full, or the aging timer (fixed to one second) of sFlow packets expires, the sFlow agent sends the sFlow packets in UDP packets to a specified sFlow collector. The sFlow collector analyzes the information and displays the results.

sFlow has the following two sampling mechanisms:

- **Flow sampling**—Obtains packet information.
- **Counter sampling**—Obtains interface counter information.

Figure 52 sFlow system



As a traffic monitoring technology, sFlow has the following advantages:

- Supports traffic monitoring on Gigabit and higher-speed networks.
- Provides good scalability to allow one sFlow collector to monitor multiple sFlow agents.
- Saves money by embedding the sFlow agent in a device, instead of using a dedicated sFlow agent device.

NOTE:

The switch only supports the sFlow agent function .

sFlow configuration task list

Task	Remarks
Configuring the sFlow agent and sFlow collector	Required.
Configuring flow sampling	Perform at least one of the tasks.
Configuring counter sampling	

Configuring the sFlow agent and sFlow collector

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify the IP address for the sFlow agent.	sflow agent { ip <i>ip-address</i> ipv6 <i>ipv6-address</i> }	<p>Optional</p> <p>Not specified by default. The device periodically checks the existence of the sFlow agent address. If the sFlow agent has no IP address configured, the device automatically selects an interface IP address for the sFlow agent but does not save the selected IP address.</p> <p>NOTE:</p> <ul style="list-style-type: none"> HP recommends configuring an IP address manually for the sFlow agent. Only one IP address can be specified for the sFlow agent on the device.
3. Configure the sFlow collector.	sflow collector <i>collector-id</i> { { ip <i>ip-address</i> ipv6 <i>ipv6-address</i> } datagram-size <i>size</i> description <i>text</i> port <i>port-number</i> time-out <i>seconds</i> } *	<p>By default, the device presets a number of sFlow collectors.</p> <p>Use the display sflow command to display the parameters of the preset sFlow collectors.</p>
4. Specify the source IP address of sent sFlow packets.	sflow source { ip <i>ip-address</i> ipv6 <i>ipv6-address</i> } *	<p>Optional</p> <p>Not specified by default.</p>

Configuring flow sampling

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Set the Flow sampling mode.	sflow sampling-mode { determine random }	<p>Optional</p> <p>random by default.</p>
4. Set the interval for flow sampling.	sflow sampling-rate <i>interval</i>	Not set by default.
5. Set the maximum copied length of a sampled packet.	sflow flow max-header <i>length</i>	<p>Optional</p> <p>By default, up to 128 bytes of a sampled packet can be copied. You are recommended to use the default value.</p>
6. Specify the sFlow collector for flow sampling.	sflow flow collector <i>collector-id</i>	No collector is specified for flow sampling by default.

NOTE:

The switch does not support the flow sampling mode **determine**.

Configuring counter sampling

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Set the interval for counter sampling.	sflow counter interval <i>seconds</i>	Counter sampling is disabled by default.
4. Specify the sFlow collector for counter sampling.	sflow counter collector <i>collector-id</i>	No collector is specified for counter sampling by default.

Displaying and maintaining sFlow

Task	Command	Remarks
Display sFlow configuration information.	display sflow [<i>slot slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view

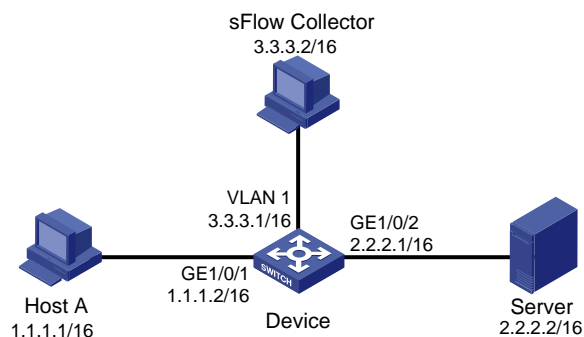
sFlow configuration example

Network requirements

As shown in [Figure 53](#), Host A is connected with the server through the device (sFlow agent).

Enable sFlow (including flow sampling and counter sampling) on GigabitEthernet 1/0/1 to monitor traffic on the interface. The device sends sFlow packets through GigabitEthernet 1/0/3 to the sFlow collector, which analyzes the sFlow packets and displays results.

Figure 53 Network diagram



Configuration procedure

1. Configure the sFlow agent and sFlow collector:

Configure the IP address of vlan-interface 1 on Device as 3.3.3.1/16.

```
<Device> system-view
[Device] interface vlan-interface 1
[Device-Vlan-interface1] ip address 3.3.3.1 16
[Device-Vlan-interface1] quit
```

Specify the IP address for the sFlow agent.

```
[Device] sflow agent ip 3.3.3.1
```

Specify sFlow collector ID 2, IP address 3.3.3.2, the default interface number, and description of **netserver** for the sFlow collector.

```
[Device] sflow collector 2 ip 3.3.3.2 description netserver
```

2. Configure counter sampling:

Set the counter sampling interval to 120 seconds.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] sflow counter interval 120
```

Specify sFlow collector 2 for counter sampling.

```
[Device-GigabitEthernet1/0/1] sflow counter collector 2
```

3. Configure flow sampling:

Set the Flow sampling mode and sampling interval.

```
[Device-GigabitEthernet1/0/1] sflow sampling-mode random
[Device-GigabitEthernet1/0/1] sflow sampling-rate 4000
```

Specify sFlow collector 2 for flow sampling.

```
[Device-GigabitEthernet1/0/1] sflow flow collector 2
```

Display the sFlow configuration and operation information.

```
[Device-GigabitEthernet1/0/1] display sflow
```

sFlow Version: 5

sFlow Global Information:

Agent IP:3.3.3.1(CLI)

Collector Information:

ID	IP	Port	Aging	Size	Description
1		6343	0	1400	
2	3.3.3.2	6543	N/A	1400	netserver
3		6343	0	1400	
4		6343	0	1400	
5		6343	0	1400	
6		6343	0	1400	
7		6343	0	1400	
8		6343	0	1400	
9		6343	0	1400	
10		6343	0	1400	

sFlow Port Information:

Interface	CID	Interval(s)	FID	MaxHLen	Rate	Mode	Status
GE1/0/1	2	120	2	128	4000	Random	Active

The output shows that GigabitEthernet 1/0/1 enabled with sFlow is active, the counter sampling interval is 120 seconds, the Flow sampling interval is 4000, all of which indicate sFlow operates normally.

Troubleshooting sFlow configuration

Symptom

The remote sFlow collector cannot receive sFlow packets.

Analysis

- The sFlow collector has no IP address specified.
- No interface is enabled with sFlow to sample data.
- The IP address of the sFlow collector specified on the sFlow agent is different from that of the remote sFlow collector.
- No IP address is configured for the Layer 3 interface on the device, or the IP address is configured, but the UDP packets with the IP address being the source cannot reach the sFlow collector.
- The physical link between the device and the sFlow collector fails.

Solution

1. Check whether sFlow is correctly configured by displaying sFlow configuration with the **display sflow** command.
2. Check whether the correct IP address is configured for the device to communicate with the sFlow collector.
3. Check whether the physical link between the device and the sFlow collector is normal.

Configuring IPC

This chapter provides an overview of Inter-Process Communication (IPC) and describes the IPC monitoring commands.

Overview

IPC provides a reliable communication mechanism among processing units, typically CPUs. IPC is typically used on a distributed device or in an IRF fabric to provide reliable inter-card or inter-device transmission. This section describes the basic IPC concepts.

Node

An IPC node is an independent IPC-capable processing unit, typically, a CPU.

The device is a centralized device that has only one CPU. The IRF fabrics formed by them have multiple CPUs, or IPC nodes.

Link

An IPC link is a connection between any two IPC nodes. Any two IPC nodes have one and only one IPC link for sending and receiving packets. All IPC nodes are fully meshed.

IPC links are created when the system is initialized. An IPC node, upon startup, sends handshake packets to other nodes. If the handshake succeeds, a connection is established.

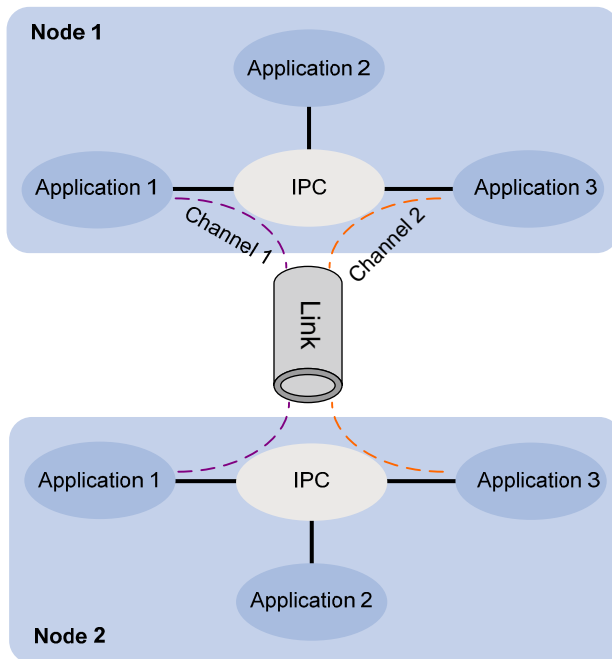
The system uses link status to identify the link connectivity between two nodes. An IPC node can have multiple links, and each link has its own status.

Channel

A channel is the communication interface between peer upper layer application modules that use different IPC nodes. Each node assigns a locally unique channel number to each upper layer application module for identification.

An upper layer application module sends data to an IPC module in a channel, and the IPC module sends the data to a peer node across a link, as shown in [Figure 54](#).

Figure 54 Relationship between a node, link and channel



Packet sending modes

IPC uses one of the following modes to send packets for upper layer application modules:

- **Unicast**—One node sends packets to another node.
- **Multicast**—One node sends packets to multiple nodes. This mode includes broadcast, a special multicast. To use multicast mode, an application module must create a multicast group that includes a set of nodes. Multicasts destined for this group are sent to all the nodes in the group. An application module can create multiple multicast groups. Creation and deletion of a multicast group or group member depend on the application module.
- **Mixcast**—Supports both unicast and multicast.

IPC assigns one queue for each mode. An upper layer application module automatically selects one mode as needed.

Enabling IPC performance statistics

The IPC performance statistics function provides the most recent 10-second, 1-minute, and 5-minute traffic input and output statistics for IPC nodes. If this function is disabled, the **display ipc performance** command displays the statistics collected before IPC performance statistics was disabled.

Perform the following task in user view:

Task	Command	Remarks
Enable IPC performance statistics.	ipc performance enable { node <i>node-id</i> self-node } [channel <i>channel-id</i>]	By default, the function is disabled.

Displaying and maintaining IPC

Task	Command	Remarks
Display IPC node information.	display ipc node [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display channel information for a node.	display ipc channel { node <i>node-id</i> self-node } [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display queue information for a node.	display ipc queue { node <i>node-id</i> self-node } [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display multicast group information for a node.	display ipc multicast-group { node <i>node-id</i> self-node } [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display packet information for a node.	display ipc packet { node <i>node-id</i> self-node } [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display link status information for a node.	display ipc link { node <i>node-id</i> self-node } [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display IPC performance statistics for a node.	display ipc performance { node <i>node-id</i> self-node } [channel <i>channel-id</i>] [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Clear IPC performance statistics for a node.	reset ipc performance [node <i>node-id</i> self-node] [channel <i>channel-id</i>]	Available in user view.

Configuring PoE

Overview

IEEE 802.3af/802.3at-compliant power over Ethernet (PoE) enables a power sourcing equipment (PSE) to supply power to powered devices (PDs) through Ethernet interfaces over straight-through twisted pair cables. Examples of PDs include IP telephones, wireless APs, portable chargers, card readers, Web cameras, and data collectors. A PD can also use a different power source from the PSE at the same time for power redundancy.

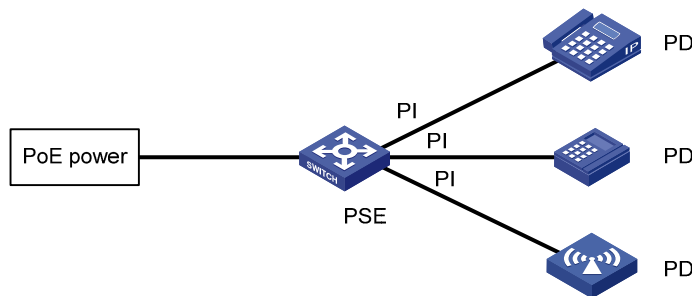
As shown in [Figure 55](#), a PoE system comprises the following elements:

- **PoE power**—The entire PoE system is powered by the PoE power.
- **PSE**—The PSE supplies power for PDs. A PSE can examine the Ethernet cables connected to PoE interfaces, search for PDs, classify them, and supply power to them. When detecting that a PD is unplugged, the PSE stops supplying power to the PD. A PSE can be built-in (Endpoint) or external (Midspan). The switch uses built-in PSEs. To display the mapping between a PSE ID and the slot number of an interface card, execute the **display poe device** command.

The PSE ID is the *switch member ID* $\times 3 + 1$. For example, if the member ID of the device is 3, the PSE ID of the device is $3 \times 3 + 1 = 10$.

- **PI**—An Ethernet interface with the PoE capability is called PoE interface.
- **PD**—A PD receives power from the PSE. You can also connect a PD to a redundant power source for reliability.

Figure 55 PoE system diagram



PoE configuration task list

You can configure PoE settings directly on a PoE interface or by configuring a PoE profile and applying the PoE profile to PoE interfaces.

PoE profile enables you to apply a set of PoE settings to multiple interfaces instead of configuring the interfaces one by one.

When configuring, removing, or deleting a PoE parameter on a PoE interface, you can use either method but not both.

Configuration guidelines

- Before configuring PoE, make sure the PoE power supply and PSE are operating correctly so you can configure PoE and the configured PoE settings can take effect.
- If the PoE power supply is turned off while the device is starting up, the PoE configuration in the PoE profile might become invalid.

Complete these tasks to configure PoE:

Task	Remarks
<ul style="list-style-type: none">• Enabling PoE for a PoE interface	Required.
Detecting PDs:	
<ul style="list-style-type: none">• Enabling the PSE to detect nonstandard PDs• Configuring a PD disconnection detection mode	Optional.
<ul style="list-style-type: none">• Configuring the maximum PoE interface power	Optional.
<ul style="list-style-type: none">• Configuring PoE interface power management	Optional.
Configuring the PoE monitoring function:	Optional.
<ul style="list-style-type: none">• Configuring PSE power monitoring• Monitoring PD	The device automatically monitors PDs when supplying power to them.
Configuring PoE interface through PoE profile:	
<ul style="list-style-type: none">• Configuring PoE profile• Applying a PoE profile	Optional.
Upgrading PSE processing software in service	Optional.

Enabling PoE for a PoE interface

The system does not supply power to or reserve power for the PDs connected to a PoE interface unless the PoE interface is enabled with the PoE function.

You can enable PoE for a PoE interface if the PoE interface does not result in PoE power overload. Otherwise, whether you can enable PoE for the PoE interface depends on whether the PoE interface is enabled with the PoE power management function. For more information about PoE interface power management, see "[Configuring PoE interface power management](#)."

- If the PoE interface is not enabled with the PoE power management function, you cannot enable PoE for the PoE interface.
- If the PoE interface is enabled with the PoE power management function, you can enable PoE for the PoE interface. Whether the PDs can be powered depends on other factors, such as the power supply priority of the PoE interface.

The PSE supplies power over category 3/5 twisted pair cable for a PoE interface in the following modes:

- **Over signal wires**—The PSE uses data pairs (pins 1, 2 and 3, 6) to supply DC power to PDs.
- **Over spare wires**—The PSE uses spare pairs (pins 4, 5 and 7, 8) to supply DC power to PDs.

When the sum of the power consumption of all powered PoE interfaces on a PSE exceeds the maximum power of the PSE, the system considers the PSE as overloaded. The maximum PSE power is user configurable.

A PSE can supply power to a PD only when the selected power supply mode is supported by both the PSE and PD. If the PSE and PD support different power supply modes (for example, the PSE does not support power over spare wires, while the PD supports power over spare wires), you have to change the order of the lines in the twisted pair cable to supply power to the PD.

The switch's PoE interfaces can supply power only over signal wires.

To enable PoE for a PoE interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter PoE interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable PoE for the PoE interface.	poe enable	By default, this function is disabled.
4. Configure a description for the PD connected to the PoE interface.	poe pd-description <i>text</i>	Optional. By default, no description for the PD connected to the PoE interface is available.

Detecting PDs

Enabling the PSE to detect nonstandard PDs

There are standard PDs and nonstandard PDs. Usually, the PSE can detect only standard PDs and supply power to them. The PSE can detect nonstandard PDs and supply power to them only if you enable the PSE to detect nonstandard PDs.

To enable the PSE to detect nonstandard PDs:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the PSE to detect nonstandard PDs.	poe legacy enable pse <i>pse-id</i>	By default, the PSE can detect only standard PDs.

Configuring a PD disconnection detection mode

CAUTION:

If you change the PD disconnection detection mode while the device is running, the connected PDs are powered off.

To detect the PD connection with a PSE, PoE provides two detection modes: AC detection and DC detection. The AC detection mode uses less energy than the DC detection mode.

To configure a PD disconnection detection mode:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure a PD disconnection detection mode.	poe disconnect { ac dc }	Optional. The default PD disconnection detection mode is AC detection.

Configuring the maximum PoE interface power

The maximum PoE interface power is the maximum power that the PoE interface can provide to the connected PD. If the PD requires more power than the maximum PoE interface power, the PoE interface does not supply power to the PD.

The total PoE power supplied by Ethernet ports numbered 1 through 24 is 370 W, and that supplied by Ethernet ports number 25 through 48 is 370 W.

To configure the maximum PSE power:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter PoE interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the maximum power for the PoE interface.	poe max-power <i>max-power</i>	Optional. The default is 30000 milliwatts.

Configuring PoE interface power management

The power supply priority of a PD depends on the priority of the PoE interface. In descending order, the power-supply priority levels of a PoE interface are critical, high, and low. Power supply to a PD is subject to PoE interface power management policies.

All PSEs implement the same PoE interface power management policies. In a PoE power overload condition, a PSE uses the following rules to decide whether to supply power to a PoE interface:

- If the priority-based power management is disabled for PoE interfaces, no power is supplied to the PoE interface.
- If the priority-based power management policy is enabled for PoE interfaces, low-priority PoE interfaces are disconnected to guarantee power for high-priority and critical-priority PoE interfaces.

The guaranteed remaining PoE power is the maximum PoE power minus the power allocated to the critical PoE interface, regardless of whether PoE is enabled for the PoE interface. If this is lower than the maximum power of the PoE interface, you cannot set the power priority of the PoE interface to **critical**. Otherwise, you can set the power priority to **critical**, and this PoE interface preempts the power of the PoE interface that has a lower priority level. In this case, the PoE interface whose power is preempted is disconnected, but its configuration remains unchanged. If you change the priority of the PoE interface from **critical** to a lower level, the PDs connecting to other PoE interfaces have an opportunity to be powered.

A guard band of 19 watts is reserved for each PoE interface on the device to prevent a PD from being powering off because of a sudden increase of power. If the remaining power of the PSE is lower than 19

watts and no priority is configured for a PoE interface, the PSE does not supply power to the new PD. If the remaining power of the PSE is lower than 19 watts, but priorities are configured for PoE interfaces, the PoE interface that has a higher priority can preempt the power of a PoE interface that has a lower priority to ensure normal operation of the higher priority PoE interface.

If a sudden increase of the PD power results in PSE power overload, power supply to the PD on the PoE interface that has a lower priority is stopped to ensure power supply to the PD that has a higher priority.

Configuration prerequisites

Enable PoE for PoE interfaces.

Configuration procedure

To configure PoE interface power management:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the priority-based power management policy for PoE interfaces.	poe pd-policy priority	By default, this policy is disabled.
3. Enter PoE interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Configure the power supply priority for a PoE interface.	poe priority { critical high low }	Optional. By default, low is the power supply priority for the PSE.

Configuring the PoE monitoring function

With the PoE monitoring function enabled, the system monitors the parameter values related to PoE power supply, PSE, PD, and device temperature in real time. When a specific value exceeds the limited range, the system automatically takes self-protection measures.

Configuring PSE power monitoring

When the PSE power exceeds or drops below the specified threshold, the system sends trap messages.

To configure a power alarm threshold for the PSE:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure a power alarm threshold for the PSE.	poe utilization-threshold <i>utilization-threshold-value</i> pse <i>pse-id</i>	Optional. The default setting is 80%.

Monitoring PD

When a PSE starts or ends power supply to a PD, the system sends a trap message.

Configuring PoE interface through PoE profile

You can configure a PoE interface either at the CLI or by using a PoE profile and applying the PoE profile to the PoE interface.

To configure a single PoE interface, configure it at the CLI. To configure PoE interfaces in batches, use a PoE profile.

A PoE profile is a collection of configurations that contain multiple PoE features. On large-scale networks, you can apply a PoE profile to multiple PoE interfaces, and these interfaces have the same PoE features. If the PoE interface connecting to a PD changes to another one, apply the PoE profile applied on the originally connected interface to the currently connected interface instead of reconfiguring the features defined in the PoE profile one by one, simplifying the PoE configurations.

The device supports multiple PoE profiles. You can define PoE configurations based on each PD, save the configurations for different PDs into different PoE profiles, and apply the PoE profiles to the access interfaces of PDs accordingly.

Configuring PoE profile

If a PoE profile is applied, it cannot be deleted or modified before you cancel its application.

The **poe max-power** *max-power* and **poe priority** { **critical** | **high** | **low** } commands must be configured in only one way, that is, either at the CLI or by configuring PoE profile.

A PoE parameter on a PoE interface must be configured, modified and deleted in only one way. If a parameter configured in a way (for example, at the CLI) is then configured in the other way (for example, through PoE profile), the latter configuration fails and the original one is still effective. To make the latter configuration effective, you must cancel the original one first.

To configure a PoE profile:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a PoE profile, and enter PoE profile view.	poe-profile <i>profile-name</i> [<i>index</i>]	N/A
3. Enable PoE for the PoE interface.	poe enable	By default, this function is disabled.
4. Configure the maximum power for the PoE interface.	poe max-power <i>max-power</i>	Optional. The default is 30000 milliwatts.
5. Configure power supply priority for the PoE interface.	poe priority { critical high low }	Optional. By default, low is the power supply priority for the PoE interface.

Applying a PoE profile

You can apply a PoE profile in either system view or interface view. If you perform application to a PoE interface in both views, the latter application takes effect. To apply a PoE profile to multiple PoE interfaces, the system view is more efficient.

A PoE profile can apply to multiple PoE interfaces, but a PoE interface can have only one PoE profile.

To apply a PoE profile to multiple interfaces in system view:

Step	Command
1. Enter system view.	system-view
2. Apply a PoE profile to one or multiple PoE interfaces.	apply poe-profile { index <i>index</i> name <i>profile-name</i> } interface <i>interface-range</i>

To apply a PoE profile to an interface in interface view:

Step	Command
1. Enter system view.	system-view
2. Enter PoE interface view.	interface <i>interface-type interface-number</i>
3. Apply a PoE profile to the PoE interface.	apply poe-profile { index <i>index</i> name <i>profile-name</i> }

Upgrading PSE processing software in service

You can upgrade the PSE processing software in service in either of the following two modes:

- **Refresh mode**—Enables you to update the PSE processing software without deleting it. Normally, you can upgrade the PSE processing software in the refresh mode through the command line.
- **Full mode**—Deletes the PSE processing software and reloads it. If the PSE processing software is damaged (in this case, you can execute none of PoE commands successfully), you can upgrade the PSE processing software in full mode to restore the PSE function.

An in-service PSE processing software upgrade may be unexpectedly interrupted (for example, an error results in device reboot). If you fail to upgrade the PSE processing software in full mode after reboot, you can power off the device and restart it before upgrading it in full mode again. After upgrade, restart the device manually to make the new PSE processing software take effect.

To upgrade the PSE processing software in service:

Step	Command
1. Enter system view.	system-view
2. Upgrade the PSE processing software in service.	poe update { full refresh } <i>filename</i> pse <i>pse-id</i>

Displaying and maintaining PoE

Task	Command	Remarks
Display PSE information.	display poe device [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the power supplying state of the specified PoE interface.	display poe interface [<i>interface-type interface-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

Task	Command	Remarks
Display power information for PoE interfaces.	display poe interface power [<i>interface-type interface-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display information about PSE.	display poe pse [<i>pse-id</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the power supply states of all PoE interfaces connected to the PSE.	display poe pse pse-id interface [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display power information for all PoE interfaces connected to the PSE.	display poe pse pse-id interface power [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the configurations and applications of the PoE profile.	display poe-profile [<i>index index</i> <i>name profile-name</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the configurations and applications of the PoE profile applied to the specified PoE interface.	display poe-profile interface <i>interface-type interface-number</i> [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

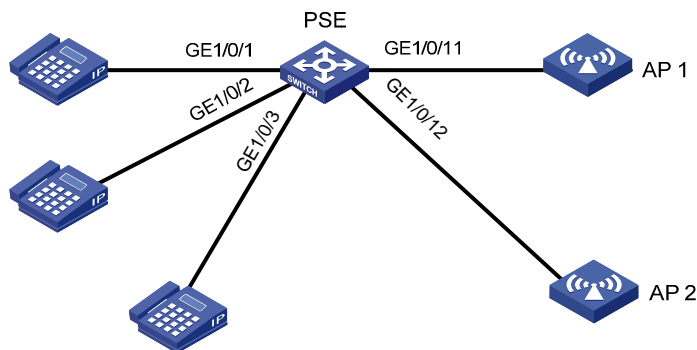
PoE configuration example

Network requirements

As shown in Figure 56, the device supplies power to PDs through its PoE interfaces:

- GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 are connected to IP telephones.
- GigabitEthernet 1/0/11 and GigabitEthernet 1/0/12 are connected to APs.
- The power supply priority of IP telephones is higher than that of the APs, for which the PSE supplies power to IP telephones first when the PSE power is overloaded.
- The maximum power of AP2 connected to GigabitEthernet 1/0/12 does not exceed 9000 milliwatts.

Figure 56 Network diagram



Configuration procedure

Enable PoE and specify the **critical** power supply priority on GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe enable
[Sysname-GigabitEthernet1/0/1] poe priority critical
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] poe enable
[Sysname-GigabitEthernet1/0/2] poe priority critical
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] poe enable
[Sysname-GigabitEthernet1/0/3] poe priority critical
[Sysname-GigabitEthernet1/0/3] quit
```

Enable PoE on GigabitEthernet 1/0/11 and GigabitEthernet 1/0/12, and configure the maximum power of GigabitEthernet 1/0/12 as 9000 milliwatts.

```
[Sysname] interface gigabitethernet 1/0/11
[Sysname-GigabitEthernet1/0/11] poe enable
[Sysname-GigabitEthernet1/0/11] quit
[Sysname] interface gigabitethernet 1/0/12
[Sysname-GigabitEthernet1/0/12] poe enable
[Sysname-GigabitEthernet1/0/12] poe max-power 9000
```

Troubleshooting PoE

Setting the priority of a PoE interface to critical fails

Analysis

- The guaranteed remaining power of the PSE is lower than the maximum power of the PoE interface.
- The priority of the PoE interface is already set.

Solution

- In the first case, either increase the maximum PSE power or reduce the maximum power of the PoE interface if the guaranteed remaining power of the PSE cannot be modified.
- In the second case, remove the priority that is already configured.

Failure to apply a PoE profile to a PoE interface

Analysis

- Some configurations in the PoE profile are already configured.
- Some configurations in the PoE profile do not meet the configuration requirements of the PoE interface.
- Another PoE profile is already applied to the PoE interface.

Solution

- In the first case, remove the original configurations of those configurations.
- In the second case, modify the configurations in the PoE profile.
- In the third case, remove the application of the undesired PoE profile to the PoE interface.

Configuring cluster management

Cluster management is supported only in non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

Overview

Cluster management is an effective way to manage large numbers of dispersed switches in groups. Cluster management offers the following advantages:

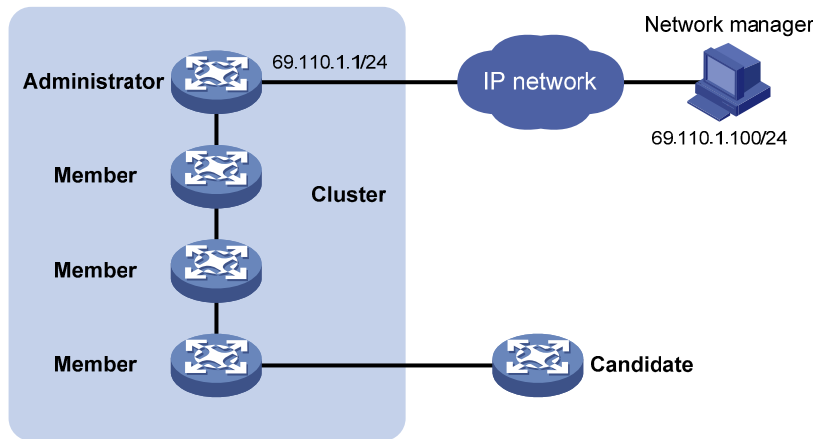
- Saves public IP address resources. You do not need to assign one public IP address for every cluster member switch.
- Simplifies configuration and management tasks. By configuring a public IP address on one switch, you can configure and manage a group of switches without the trouble of logging in to each switch separately.
- Provides a useful topology discovery and display function for network monitoring and debugging.
- Allows simultaneous software upgrading and parameter configuration on multiple switches, free from topology and distance limitations.

Roles in a cluster

The switches in a cluster play different roles according to their different functions and status. You can specify the following roles for the switches:

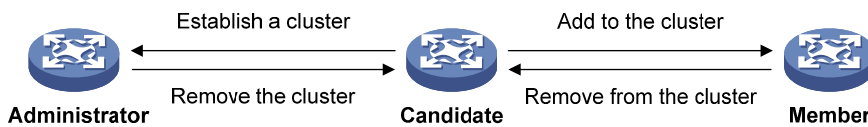
- **Management device (Administrator)**—A switch that provides management interfaces for all switches in a cluster and the only switch configured with a public IP address. You can specify one and only one management switch for a cluster. Any configuration, management, and monitoring of the other switches in a cluster can be implemented only through the management switch. The management switch collects topology data to discover and define candidate switches.
- **Member device (Member)**—A switch managed by the management switch in a cluster.
- **Candidate device (Candidate)**—A switch that does not yet belong to any cluster but can be added to a cluster. Different from a member switch, its topology information has been collected by the management switch but it has not been added to the cluster.

Figure 57 Network diagram



As shown in [Figure 57](#), the switch configured with a public IP address and performing the management function is the management switch, the other managed switches are member switches, and the switch that does not belong to any cluster but can be added to a cluster is a candidate switch. The management switch and the member switches form the cluster.

Figure 58 Role change in a cluster



As shown in [Figure 58](#), a switch in a cluster changes its role according to the following rules:

- A candidate switch becomes a management switch when you create a cluster on it. A management switch becomes a candidate switch only after the cluster is removed.
- A candidate switch becomes a member switch after it is added to a cluster. A member switch becomes a candidate switch after it is removed from the cluster.

How a cluster works

Cluster management is implemented through HW Group Management Protocol version 2 (HGMPv2), which consists of the following three protocols:

- Neighbor Discovery Protocol (NDP)
- Neighbor Topology Discovery Protocol (NTDP)
- Cluster

These protocols enable topology data collection and cluster establishment and maintenance.

The following is the topology data collection process:

- Every switch uses NDP to collect data on the directly connected neighbors, including their software version, host name, MAC address and port number.
- The management switch uses NTDP to collect data on the switches within user-specified hops and their topology data, and identifies candidate switches based on the topology data.
- The management switch adds or deletes a member switch and modifies the cluster management configuration according to the candidate switch information collected through NTDP.

About NDP

NDP discovers information about directly connected neighbors, including the switch name, software version, and connecting port of the adjacent switches. NDP works in the following ways:

- A switch running NDP periodically sends NDP packets to its neighbors. An NDP packet carries NDP information (including the switch name, software version, and connecting port) and the holdtime. The holdtime indicates how long the receiving switches will keep the NDP information. At the same time, the switch also receives, but does not forward, NDP packets from its neighbors.
- A switch running NDP stores and maintains an NDP table. The switch creates an entry in the NDP table for each neighbor. If a new neighbor is found, meaning the switch receives an NDP packet sent by the neighbor for the first time, the switch adds an entry to the NDP table. If the NDP information carried in the NDP packet is different from the stored information, the corresponding entry and holdtime in the NDP table are updated. Otherwise, only the holdtime of the entry is updated. If no NDP information is received from the neighbor when the holdtime times out, the corresponding entry is removed from the NDP table.

NDP runs on the data link layer and supports different network layer protocols.

About NTDP

NTDP provides information required for cluster management. It collects topology information about the switches within the specified hop count. Based on the neighbor information stored in the neighbor table maintained by NDP, NTDP on the management switch advertises NTDP topology-collection requests to collect the NDP information of all the switches in a specific network range as well as the connection information of all its neighbors. The information collected will be used by the management switch or the network management software to implement required functions.

When a member switch detects a change on its neighbors through its NDP table, it informs the management switch through handshake packets. Then the management switch triggers its NTDP to collect specific topology information, so that its NTDP can discover topology changes promptly.

The management switch collects topology information periodically. You can also administratively launch a topology information collection. The process of topology information collection is as follows:

- The management switch periodically sends NTDP topology-collection request from the NTDP-enabled ports.
- Upon receiving the request, the switch sends NTDP topology-collection response to the management switch, copies this response packet on the NTDP-enabled port, and sends it to the adjacent switch. Topology-collection response includes the basic information of the NDP-enabled switch and NDP information of all adjacent switches.
- The adjacent switch performs the same operation until the NTDP topology-collection request is sent to all the switches within specified hops.

To avoid concurrent responses to an NTDP topology-collection request causing congestion and deny of service on the management switch, a delay mechanism was introduced. You configure the delay parameters for NTDP on the management switch. As a result:

- Each requested switch waits for a period of time before forwarding an NTDP topology-collection request on the first NTDP-enabled port.
- After the first NTDP-enabled port forwards the request, all other NTDP-enabled ports on the requested switch forward the request in turn at a specific interval.

Cluster management maintenance

1. Adding a candidate switch to a cluster:

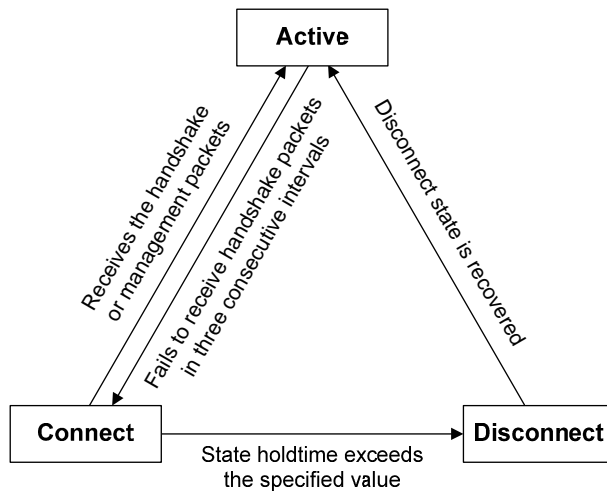
You should specify the management switch before creating a cluster. The management switch discovers and defines a candidate switch through NDP and NTDP protocols. The candidate switch can be automatically or manually added to the cluster.

After the candidate switch is added to the cluster, it can obtain the member number assigned by the management switch and the private IP address used for cluster management.

2. Communication within a cluster:

In a cluster the management switch communicates with its member switches by sending handshake packets to maintain connection between them. The management/member switch state change is shown in Figure 59.

Figure 59 Management/member switch state change



A cluster manages the state of its member switches as follows:

- After a candidate switch is added to the cluster and becomes a member switch, the management switch saves its state information and identifies it as Active. The member switch also saves its state information and identifies itself as Active.
- The management switch and member switches send handshake packets. Upon receiving the handshake packets, the management switch or a member switch keeps its state as Active without sending a response.
- If the management switch does not receive handshake packets from a member switch within a period that is three times the handshake interval, it changes the status of the member switch from Active to Connect. Likewise, if a member switch fails to receive handshake packets within a period that is three times the handshake interval, its state changes from Active to Connect.
- During the information holdtime, if the management switch receives handshake or management packets from a member switch that is in Connect state, it changes the state of the member switch to Active. Otherwise, it considers the member switch to be disconnected, and changes the state of the member switch to Disconnect.
- During the information holdtime, a member switch in Connect state changes its state to Active if it receives handshake or management packets from the management switch. Otherwise, it changes its state to Disconnect.
- When the communication between the management switch and a member switch is recovered, the member switch is added to the cluster and its state changes from Disconnect to Active on itself and the management switch.
- Also, a member switch sends handshake packets to inform the management switch of neighbor

topology changes.

Management VLAN

Management VLAN limits the cluster boundaries. All cluster control packets, including NDP, NTDP, and handshake packets between the management switch and member switches are restricted within the cluster management VLAN.

To assign a candidate to a cluster, make sure all ports on the path from the candidate switch to the management switch are in the management VLAN. If not, the candidate switch cannot join the cluster.

You can manually assign ports to the management VLAN or use the management VLAN autonegotiation function to enable automatic VLAN assignment on the management switch.

❗ IMPORTANT:

To guarantee the communication within the cluster, ensure VLAN handling consistency on all ports on the path from a member switch or candidate switch to the management switch. To remove the VLAN tag of outgoing management VLAN packets, set the management VLAN as the PVID on all the ports, including hybrid ports. If the management VLAN is not the PVID, a hybrid and trunk port must send outgoing management VLAN packets with the VLAN tag.

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

Configuration restrictions and guidelines

- Do not disable NDP or NTDP after a cluster is formed. Doing so on the cluster management switch or its member switches does not break up the cluster, but can affect operation of the cluster.
- If an 802.1X- or MAC authentication-enabled member switch is connected to any other member switch, enable HABP server on the switch. Otherwise, the management switch of the cluster cannot manage the switches connected to it. For more information about HABP, see *Security Configuration Guide*.
- Before you establish a cluster or add a switch to the cluster, verify that:
 - The management switch's routing table can accommodate routes destined for the candidate switches. A full routing table can cause continual additions and removals of all candidate switches.
 - The candidate switch's routing table can accommodate the route destined for the management switch. A full routing table can cause continual additions and removals of the candidate switch.

Cluster management configuration task list

Before configuring a cluster, determine the roles and functions the switches play, and configure functions required for the cluster member switches to communicate with one another.

Complete these tasks to configure cluster management functions:

Task	Remarks
Configuring the management switch:	
• Enabling NDP globally and for specific ports	Required.
• Configuring NDP parameters	Optional.
• Enabling NTDP globally and for specific ports	Required.

Task	Remarks
• Configuring NTDP parameters	Optional.
• Manually collecting topology information	Optional.
• Enabling the cluster function	Required.
• Establishing a cluster	Required.
• Enabling management VLAN autonegotiation	Required.
• Configuring communication between the management switch and the member switches within a cluster	Optional.
• Configuring cluster management protocol packets	Optional.
• Cluster member management	Optional.
Configuring the member switches:	
• Enabling NDP	Optional.
• Enabling NTDP	Optional.
• Manually collecting topology information	Optional.
• Enabling the cluster function	Optional.
• Deleting a member switch from a cluster	Optional.
• Toggling between the CLIs of the management switch and a member switch	Optional.
• Adding a candidate switch to a cluster	Optional.
Configuring advanced cluster management functions:	
• Configuring topology management	Optional.
• Configuring interaction for a cluster	Optional.
• Configuring the SNMP configuration synchronization function	Optional.
• Configuring Web user accounts in batches	Optional.

Configuring the management switch

Perform the tasks in this section on the management switch.

Enabling NDP globally and for specific ports

For NDP to work normally, enable NTDP both globally and on specific ports.

To enable NDP globally and for specific ports:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable NDP globally.	ndp enable	Optional. By default, this function is disabled.

Step	Command	Remarks
3. Enable NDP on ports.	<ul style="list-style-type: none"> In system view: ndp enable interface <i>interface-list</i> In Ethernet interface view or Layer 2 aggregate interface view: <ul style="list-style-type: none"> a. interface <i>interface-type</i> <i>interface-number</i> b. ndp enable 	<p>Use either command.</p> <p>By default, NDP is disabled globally and also on all ports.</p> <p>To avoid the management switch collecting unnecessary topology data, disable NDP on ports connected to non-candidate switches.</p>

Configuring NDP parameters

An NDP-enabled port periodically sends NDP packets that have an aging time. If the receiving device has not received any NDP packet before that aging time expires, the receiving device automatically removes the neighbor entry for the sending device.

To avoid NDP table entry flappings, make sure the NDP aging timer is equal to or longer than the NDP packet sending interval.

To configure NDP parameters:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the interval for sending NDP packets.	ndp timer hello <i>hello-time</i>	Optional. The default interval is 60 seconds.
3. Configure the period for the receiving switch to keep the NDP packets.	ndp timer aging <i>aging-time</i>	Optional. The default setting is 180 seconds.

Enabling NTDP globally and for specific ports

For NTDP to work normally, you must enable NTDP both globally and on specific ports.

To enable NTDP globally and for specific ports:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable NTDP globally.	ntdp enable	Optional. By default, NTDP is disabled globally.
3. Enter Ethernet interface view or Layer 2 aggregate interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A

Step	Command	Remarks
		Optional. By default, NTDP is disabled on all ports.
4. Enable NTDP on the port.	ntdp enable	To avoid the management switch collecting unnecessary topology data, disable NTDP on ports connected to non-candidate switches.

Configuring NTDP parameters

NTDP parameter configuration includes the following:

- Limiting the maximum number of hops (devices) from which topology data is collected.
- Setting the topology data collection interval.
- Setting the following topology request forwarding delays for requested switches' NTDP-enabled ports:
 - Forwarding delay for the first NTDP-enabled port**—After receiving a topology request, the requested switch forwards the request out of the first NTDP-enabled port when this forwarding delay expires rather than immediately.
 - Forwarding delay for other NTDP-enabled ports**—After the first NTDP-enabled port forwards the request, all other NTDP-enabled ports forward the request in turn at this delay interval.

The delay settings are conveyed in topology requests sent to the requested switches. They help avoid concurrent responses to an NTDP topology-collection request causing congestion and deny of service on the management switch.

To configure NTDP parameters:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the maximum hops for topology collection.	ntdp hop <i>hop-value</i>	Optional. The default setting is 3.
3. Configure the interval for collecting topology information.	ntdp timer <i>interval</i>	Optional. The default interval is 1 minute.
4. Configure the delay for the first NTDP-enabled port to forward a topology-collection request.	ntdp timer hop-delay <i>delay-time</i>	Optional. The default setting is 200 ms.
5. Configure the delay for other NTDP-enabled ports to forward a topology-collection request.	ntdp timer port-delay <i>delay-time</i>	Optional. The default setting is 20 ms.

Manually collecting topology information

The management switch collects topology information periodically after a cluster is created. In addition, you can manually start topology information collection on the management switch or NTDP-enabled

switch, thus managing and monitoring switches in real time, regardless of whether a cluster is created. To configure to manually collect topology information:

Task	Command
Manually collect topology information.	ntdp explore

Enabling the cluster function

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the cluster function globally.	cluster enable	Optional. By default, this function is disabled.

Establishing a cluster

To successfully establish a cluster:

- Make sure UDP port 40000 is not used by any application. This port will be used by the cluster management module for exchanging handshake packets.
- Perform the following tasks before establishing the cluster:
 - Specify a management VLAN. You cannot change the management VLAN after a cluster is created.
 - Configure a private IP address pool on the management switch for cluster member switches. This address pool must not include IP addresses that are on the same subnet as the IP address assigned to any VLAN interface on the management switch or a cluster candidate switch. When a candidate switch is added to the cluster, the management switch assigns it a private IP address for inter-cluster communication.

A cluster can be established manually or automatically. By using the automatic setup method:

1. You enter a name for the cluster you want to establish.
2. The system lists all candidate switches within your predefined hop count.
3. The system starts to add them to the cluster.
During this process, you can press **Ctrl+C** to stop the process. However, switches already added into the cluster are not removed.

To establish a cluster:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify the management VLAN.	management-vlan <i>vlan-id</i>	Optional. By default, VLAN 1 is the management VLAN.
3. Enter cluster view.	cluster	N/A

Step	Command	Remarks
4. Configure the private IP address range for member switches.	ip-pool <i>ip-address</i> { <i>mask</i> <i>mask-length</i> }	By default, the private IP address range for member switches is not configured.
5. Establish a cluster.	<ul style="list-style-type: none"> Manually establish a cluster: build <i>cluster-name</i> Automatically establish a cluster: auto-build [<i>recover</i>] 	<p>Use either method.</p> <p>By default, the switch is not the management switch.</p>

Enabling management VLAN autonegotiation

Management VLAN limits the cluster boundaries. To assign a switch to a cluster, you must make sure the port that directly connects the switch to the management switch and its cascade ports are in the management VLAN.

Management VLAN autonegotiation enables a cluster management switch to add ports directly connected to it and cascades ports between cluster candidate switches to a management VLAN.

Enabling management VLAN autonegotiation can cause the following changes to ports connecting member switches:

- Access ports change to hybrid ports. These hybrid ports permit only the management VLAN to pass through and are tagged members in the management VLAN.
- Trunk and hybrid ports are assigned to the management VLAN, without any link type or removal of VLANs that have added on the ports. Hybrid ports are added to the management VLAN as a tagged member.

Before enabling the function, make sure you fully understand its impact on your network.

To enable management VLAN autonegotiation on the management switch:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter cluster view.	cluster	N/A
3. Enable management VLAN autonegotiation.	management-vlan synchronization enable	By default, this function is disabled.

Configuring communication between the management switch and the member switches within a cluster

In a cluster, the management switch and its member switches communicate by sending handshake packets to maintain a connection. You can configure the interval for sending handshake packets and the holdtime of a switch on the management switch. This configuration applies to all member switches within the cluster. For a member switch in Connect state:

- If the management switch does not receive handshake packets from a member switch within the holdtime, it changes the state of the member switch to Disconnect. When the communication is recovered, the member switch needs to be re-added to the cluster (this process is automatically performed).

- If the management switch receives handshake packets from the member switch within the holdtime, the state of the member switch remains Active and the holdtime is restarted.

To configure communication between the management switch and the member switches within a cluster:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter cluster view.	cluster	N/A
3. Configure the handshake interval.	timer <i>interval</i>	Optional. The default interval is 10 seconds.
4. Configure the holdtime of a switch.	holdtime <i>hold-time</i>	Optional. The default setting is 60 seconds.

Configuring cluster management protocol packets

By default, the destination MAC address of cluster management protocol packets (including NDP, NTDP and HABP packets) is a multicast MAC address 0180-C200-000A, which IEEE reserved for later use. Since some switches cannot forward the multicast packets with the destination MAC address of 0180-C200-000A, so cluster management packets cannot traverse these switches. For a cluster to work normally in this case, you can modify the destination MAC address of a cluster management protocol packet without changing the current networking.

The management switch periodically sends MAC address negotiation broadcast packets to advertise the destination MAC address of the cluster management protocol packets.

When you configure the destination MAC address for cluster management protocol packets:

- If the interval for sending MAC address negotiation broadcast packets is 0, the system automatically sets it to 1 minute.
- If the interval for sending MAC address negotiation broadcast packets is not 0, the interval remains unchanged.

To configure the destination MAC address of the cluster management protocol packets:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter cluster view.	cluster	N/A
3. Configure the destination MAC address for cluster management protocol packets.	cluster-mac <i>mac-address</i>	By default, the destination MAC address is 0180-C200-000A. The following are the configurable MAC addresses: <ul style="list-style-type: none"> • 0180-C200-0000. • 0180-C200-000A. • 0180-C200-0020 through 0180-C200-002F. • 010F-E200-0002.

Step	Command	Remarks
4.	Configure the interval for sending MAC address negotiation broadcast packets. cluster-mac syn-interval <i>interval</i>	Optional. The default interval is one minute.

Cluster member management

You can manually add a candidate switch to a cluster, or remove a member switch from a cluster.

If a member switch needs to be rebooted for software upgrade or configuration update, you can remotely reboot it through the management switch.

Adding a member switch

Step	Command
1. Enter system view.	system-view
2. Enter cluster view.	cluster
3. Add a candidate switch to the cluster.	add-member [<i>member-number</i>] mac-address <i>mac-address</i> [password <i>password</i>]

Removing a member switch

Step	Command
1. Enter system view.	system-view
2. Enter cluster view.	cluster
3. Remove a member switch from the cluster.	delete-member <i>member-number</i> [to-black-list]

Rebooting a member switch

Step	Command
1. Enter system view.	system-view
2. Enter cluster view.	cluster
3. Reboot a specified member switch.	reboot member { <i>member-number</i> mac-address <i>mac-address</i> } [eraseflash]

Configuring the member switches

Enabling NDP

See "[Enabling NDP globally and for specific ports.](#)"

Enabling NTDP

See "Enabling NTDP globally and for specific ports."

Manually collecting topology information

See "Manually collecting topology information."

Enabling the cluster function

See "Enabling the cluster function."

Deleting a member switch from a cluster

Step	Command
1. Enter system view.	system-view
2. Enter cluster view.	cluster
3. Delete a member switch from the cluster.	undo administrator-address

Toggling between the CLIs of the management switch and a member switch

In a cluster, you can access the CLI of a member switch from the management switch or access the CLI of the management switch from a member switch.

Because CLI toggling uses Telnet, the following restrictions apply:

- Authentication is required for toggling to the management switch. If authentication is passed, you are assigned the user privilege level predefined on the management switch.
- When a candidate switch is added to the cluster, its super password for level-3 commands changes to be the same as that on the management switch. To avoid authentication failures, HP recommends you not modify the super password settings of any member (including the management switch and member switches) in the cluster.
- After toggling to a member switch, you have the same user privilege level as on the management switch.
- If the maximum number of Telnet users on the target switch has been reached, you cannot toggle to the switch.

Perform the following tasks in user view:

Task	Command	Remarks
Access the CLI of a member switch from the management switch.	cluster switch-to { <i>member-number</i> mac-address <i>mac-address</i> sysname <i>member-sysname</i> }	N/A

Task	Command	Remarks
Access the CLI of the management switch from a member switch.	cluster switch-to administrator	You can use this command only if you're not logged in to the member switch from the CLI of the management switch.

Adding a candidate switch to a cluster

Step	Command
1. Enter system view.	system-view
2. Enter cluster view.	cluster
3. Add a candidate switch to the cluster.	administrator-address mac-address name name

Configuring advanced cluster management functions

Configuring topology management

The concepts of blacklist and whitelist are used for topology management. An administrator can diagnose the network by comparing the current topology (namely, the information of a node and its neighbors in the cluster) and the standard topology.

- **Topology management whitelist (standard topology)**—A whitelist is a list of topology information that has been confirmed by the administrator as correct. You can get information about a node and its neighbors from the current topology. Based on this information, you can manage and maintain the whitelist by adding, deleting or modifying a node.
- **Topology management blacklist**—Switches in a blacklist are not allowed to join a cluster. A blacklist contains the MAC addresses of switches. If a blacklisted switch is connected to a network through another switch not included in the blacklist, the MAC address and access port of the latter are also included in the blacklist. The candidate switches in a blacklist can be added to a cluster only if the administrator manually removes them from the list.

The whitelist and blacklist are mutually exclusive. A whitelist member cannot be a blacklist member, and the blacklist member cannot be a whitelist member. However, a topology node can belong to neither the whitelist nor the blacklist. Nodes of this type are usually newly added nodes, whose identities are to be confirmed by the administrator.

You can back up and restore the whitelist and blacklist in the following two ways:

- Backing them up on the FTP server shared by the cluster. You can manually restore the whitelist and blacklist from the FTP server.
- Backing them up in the Flash of the management switch. When the management switch restarts, the whitelist and blacklist will be automatically restored from the Flash. When a cluster is re-established, you can choose whether to restore the whitelist and blacklist from the Flash automatically, or you can manually restore them from the Flash of the management switch.

To configure cluster topology management:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter cluster view.	cluster	N/A
3. Add a switch to the blacklist.	black-list add-mac <i>mac-address</i>	Optional.
4. Remove a switch from the blacklist.	black-list delete-mac { all <i>mac-address</i> }	Optional.
5. Confirm the current topology and save it as the standard topology.	topology accept { all [save-to { ftp-server local-flash }] mac-address <i>mac-address</i> member-id <i>member-number</i> }	Optional.
6. Save the standard topology to the FTP server or the local Flash.	topology save-to { ftp-server local-flash }	Optional.
7. Restore the standard topology.	topology restore-from { ftp-server local-flash }	Optional.

Configuring interaction for a cluster

You can configure shared FTP/TFTP server, NMS, and log host settings for the cluster on the management switch.

- Cluster members access the FTP/TFTP server through the management switch. When you execute the **ftp server-address** or **tftp server-address** command on a cluster member, you specify the private IP address of the management switch for the *server-address* argument to access the FTP/TFTP server. For more information about the **ftp** and **tftp** commands, see *Fundamentals Command Reference*.
- Cluster members output their log data to the management switch, which converts the IP address for the log data packets before forwarding the packets to the log host.
- Cluster member switches send their traps to the SNMP NMS through the management switch.

If the port of an access NM switch (including FTP/TFTP server, NM host and log host) does not allow the packets from the management VLAN to pass, the NM switch cannot manage the switches in a cluster through the management switch. In this case, on the management switch, you need to configure the VLAN interface of the access NM switch (including FTP/TFTP server, NM host and log host) as the NM interface.

To isolate cluster management and control packets from the external networks for security, HP recommends you configure the ports connected to the external networks as not allowing the management VLAN to pass through. If the port connected to the NMS, FTP/TFTP server, or log host is one of these ports, you must specify a VLAN interface other than the management VLAN interface as the network management interface for communicating with these devices. Otherwise, communication failure will occur.

To configure the interaction for a cluster:

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

Step		Command	Remarks
3.	Configure the FTP server shared by the cluster.	ftp-server <i>ip-address</i> [user-name <i>username</i> password { simple cipher } <i>password</i>]	By default, no FTP server is configured for a cluster.
4.	Configure the TFTP server shared by the cluster.	tftp-server <i>ip-address</i>	By default, no TFTP server is configured for a cluster.
5.	Configure the log host shared by the member switches in the cluster.	logging-host <i>ip-address</i>	By default, no log host is configured for a cluster.
6.	Configure the SNMP NM host shared by the cluster.	snmp-host <i>ip-address</i> [community-string read <i>string1</i> write <i>string2</i>]	By default, no SNMP host is configured.
7.	Configure the NM interface of the management switch.	nm-interface vlan-interface <i>interface-name</i>	Optional.

Configuring the SNMP configuration synchronization function

SNMP configuration synchronization simplifies SNMP configuration in a cluster by enabling the management switch to propagate its SNMP settings to all member switches on a whitelist. These SNMP settings are retained on the member switches after they are removed from the whitelist or the cluster is dismissed.

To configure the SNMP configuration synchronization function:

Step		Command	Remarks
1.	Enter system view.	system-view	N/A
2.	Enter cluster view.	cluster	N/A
3.	Configure the SNMP community name shared by a cluster.	cluster-snmp-agent community { read write } <i>community-name</i> [mib-view <i>view-name</i>]	N/A
4.	Configure the SNMPv3 group shared by a cluster.	cluster-snmp-agent group v3 <i>group-name</i> [authentication privacy] [read-view <i>read-view</i>] [write-view <i>write-view</i>] [notify-view <i>notify-view</i>]	N/A
5.	Create or update information about the MIB view shared by a cluster.	cluster-snmp-agent mib-view included <i>view-name</i> <i>oid-tree</i>	By default, the name of the MIB view shared by a cluster is ViewDefault and a cluster can access the ISO subtree.
6.	Add a user to the SNMPv3 group shared by a cluster.	cluster-snmp-agent usm-user v3 <i>user-name</i> <i>group-name</i> [authentication-mode { md5 sha } <i>auth-password</i>] [privacy-mode des56 <i>priv-password</i>]	N/A

Configuring Web user accounts in batches

Configuring Web user accounts in batches enables you to do the following:

- Through the Web interface, configure, on the management switch, the username and password used to log in to the cluster switches (including the management switch and member switches).
- Synchronize the configurations to the member switches on the whitelist.

This operation is equal to performing the configurations on the member switches. You need to enter your username and password when you log in to the cluster switches (including the management switch and member switches) through the Web interface.

These Web user account settings are retained on the member switches after they are removed from the whitelist or the cluster is dismissed.

To configure Web user accounts in batches:

Step	Command
1. Enter system view.	system-view
2. Enter cluster view.	cluster
3. Configure Web user accounts in batches.	cluster-local-user <i>user-name</i> password { cipher simple } <i>password</i>

Displaying and maintaining cluster management

Task	Command	Remarks
Display NDP configuration information.	display ndp [interface <i>interface-list</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display NTDP configuration information.	display ntdp [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display switch information collected through NTDP.	display ntdp device-list [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display detailed NTDP information for a specified switch.	display ntdp single-device mac-address <i>mac-address</i> [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display information about the cluster to which the current switch belongs.	display cluster [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the standard topology.	display cluster base-topology [<i>mac-address</i> <i>mac-address</i> <i>member-id</i> <i>member-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the current blacklist of the cluster.	display cluster black-list [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display information about candidate switches.	display cluster candidates [<i>mac-address</i> <i>mac-address</i> verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

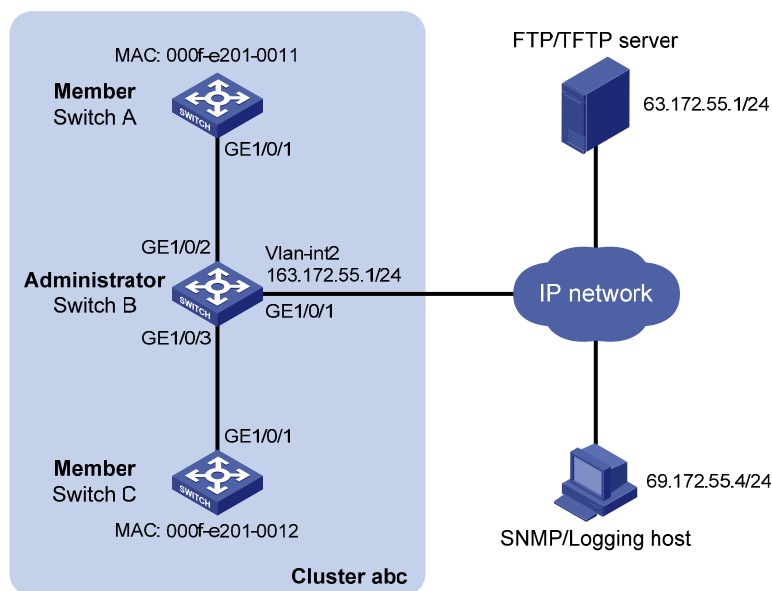
Task	Command	Remarks
Display the current topology.	display cluster current-topology [mac-address <i>mac-address</i> [to-mac-address <i>mac-address</i>] member-id <i>member-number</i> [to-member-id <i>member-number</i>]] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display information about cluster members.	display cluster members [<i>member-number</i> verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Clear NDP statistics.	reset ndp statistics [interface <i>interface-list</i>]	Available in user view.

Cluster management configuration example

Network requirements

- Three switches form cluster **abc**, whose management VLAN is VLAN 10. In the cluster, Switch B serves as the management switch (Administrator), whose network management interface is VLAN-interface 2; Switch A and Switch C are the member switches (Member).
- All the switches in the cluster use the same FTP server and TFTP server on host 63.172.55.1/24, and use the same SNMP NMS and log services on host IP address: 69.172.55.4/24.
- Add the switch whose MAC address is 000f-e201-0013 to the blacklist.

Figure 60 Network diagram



Configuration procedure

1. Configure the member switch Switch A:
Enable NDP globally and for port GigabitEthernet 1/0/1.

```
<SwitchA> system-view
[SwitchA] ndp enable
```

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] ndp enable
[SwitchA-GigabitEthernet1/0/1] quit
# Enable NTDP globally and for port GigabitEthernet 1/0/1.
[SwitchA] ntdp enable
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] ntdp enable
[SwitchA-GigabitEthernet1/0/1] quit
# Enable the cluster function.
[SwitchA] cluster enable
```

2. Configure the member switch Switch C:

As the configurations for the member switches are the same, the configuration procedure for Switch C is not shown here.

3. Configure the management switch Switch B:

Enable NDP globally and for ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
<SwitchB> system-view
[SwitchB] ndp enable
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ndp enable
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] ndp enable
[SwitchB-GigabitEthernet1/0/3] quit
```

Configure the period for the receiving switch to keep NDP packets as 200 seconds.

```
[SwitchB] ndp timer aging 200
```

Configure the interval to send NDP packets as 70 seconds.

```
[SwitchB] ndp timer hello 70
```

Enable NTDP globally and for ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
[SwitchB] ntdp enable
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ntdp enable
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] ntdp enable
[SwitchB-GigabitEthernet1/0/3] quit
```

Configure the hop count to collect topology as 2.

```
[SwitchB] ntdp hop 2
```

Configure the delay to forward topology-collection request packets on the first port as 150 ms.

```
[SwitchB] ntdp timer hop-delay 150
```

Configure the delay to forward topology-collection request packets on the first port as 15 ms.

```
[SwitchB] ntdp timer port-delay 15
```

Configure the interval to collect topology information as 3 minutes.

```
[SwitchB] ntdp timer 3
```

Configure the management VLAN of the cluster as VLAN 10.

```
[SwitchB] vlan 10
```

```

[SwitchB-vlan10] quit
[SwitchB] management-vlan 10
# Configure ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as Trunk ports and allow
packets from the management VLAN to pass.
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-type trunk
[SwitchB-GigabitEthernet1/0/3] port trunk permit vlan 10
[SwitchB-GigabitEthernet1/0/3] quit
# Enable the cluster function.
[SwitchB] cluster enable
# Configure a private IP address range for the member switches, which is from 172.16.0.1 to
172.16.0.7.
[SwitchB] cluster
[SwitchB-cluster] ip-pool 172.16.0.1 255.255.255.248
# Configure the current switch as the management switch, and establish a cluster named abc.
[SwitchB-cluster] build abc
Restore topology from local flash file,for there is no base topology.
(Please confirm in 30 seconds, default No). (Y/N)
N
# Enable management VLAN autonegotiation.
[abc_0.SwitchB-cluster] management-vlan synchronization enable
# Configure the holdtime of the member switch information as 100 seconds.
[abc_0.SwitchB-cluster] holdtime 100
# Configure the interval to send handshake packets as 10 seconds.
[abc_0.SwitchB-cluster] timer 10
# Configure the FTP Server, TFTP Server, Log host and SNMP host for the cluster.
[abc_0.SwitchB-cluster] ftp-server 63.172.55.1
[abc_0.SwitchB-cluster] tftp-server 63.172.55.1
[abc_0.SwitchB-cluster] logging-host 69.172.55.4
[abc_0.SwitchB-cluster] snmp-host 69.172.55.4
# Add the switch whose MAC address is 000f-e201-0013 to the blacklist.
[abc_0.SwitchB-cluster] black-list add-mac 000f-e201-0013
[abc_0.SwitchB-cluster] quit
# Add port GigabitEthernet 1/0/1 to VLAN 2, and configure the IP address of VLAN-interface 2.
[abc_0.SwitchB] vlan 2
[abc_0.SwitchB-vlan2] port gigabitethernet 1/0/1
[abc_0.SwitchB] quit
[abc_0.SwitchB] interface vlan-interface 2
[abc_0.SwitchB-Vlan-interface2] ip address 163.172.55.1 24
[abc_0.SwitchB-Vlan-interface2] quit
# Configure VLAN-interface 2 as the network management interface.
[abc_0.SwitchB] cluster

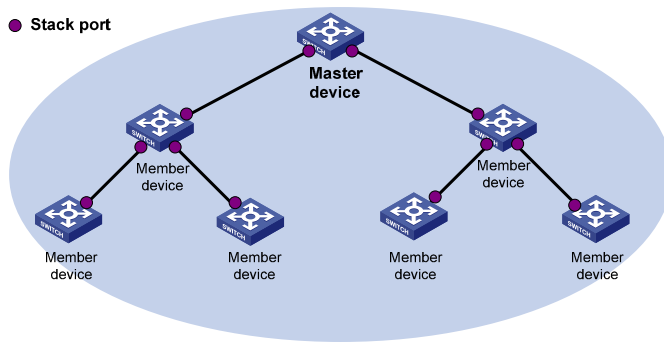
```

```
[abc_0.SwitchB-cluster] nm-interface vlan-interface 2
```


Configuring a stack

The stack management feature allows you to access a group of connected devices from one device in the group, as shown in Figure 61.

Figure 61 Network diagram for stack management



To set up a stack for a group of connected devices, you must create the stack on one device in the group. This device is the master device for the stack. Ports that connect the stack member devices are called "stack ports."

After you are logged in to the master device, you can access the CLI of any other stack member device by using a CLI switchover command.

Hardware compatibility and other restrictions

Link aggregation is not supported on stack ports. Every two stack member can have only one physical stack link between them.

Stack configuration task list

Task	Remarks
Configuring the stack master device: <ul style="list-style-type: none">Configuring a private IP address pool for the stackConfiguring stack portsCreating a stack	All these tasks are required.
Configuring stack ports on a member device	Required.
Logging in to the CLI of a member from the master	Required.

Configuring the stack master device

Perform the tasks in this section to configure the master device. After you complete the stack configuration, the master automatically adds member devices to the stack.

Always start configuring the master device with assigning a private IP address pool to the stack. You cannot perform this task after a device is configured as the master device or a member device.

Configuring a private IP address pool for the stack

Make sure the number of IP addresses in the address pool is equal to or greater than the number of devices to be added to the stack. If not, some devices cannot join the stack for lack of private IP addresses.

To configure a private IP address pool for the stack:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure a private IP address pool for the stack.	stack ip-pool <i>ip-address</i> { <i>mask</i> <i>mask-length</i> }	By default, no IP address pool is configured for a stack.

Configuring stack ports

Configure the ports that connect the master to member devices as stack ports.

To configure stack ports:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure stack ports.	stack stack-port <i>stack-port-num</i> port <i>interface-list</i>	By default, no ports are stack ports. The <i>stack-port-num</i> argument specifies the number of stack ports for the stack.

Creating a stack

After you execute the **stack role master** command, the device becomes a stack master device and automatically adds the devices connected to its stack ports to the stack.

To create a stack:

Step	Command
1. Enter system view.	system-view
2. Create a stack.	stack role master

After you configure a device as a stack master device, its CLI prompt changes to <stack_0.Sysname>, where Sysname is the system name of the device.

Configuring stack ports on a member device

To add a device to a stack, you must configure the ports that connect the device to other stack members (including the master) as stack ports.

Perform this task on each stack member device.

To configure stack ports:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure stack ports.	stack stack-port <i>stack-port-num</i> port <i>interface-list</i>	By default, a port is not a stack port.

After a device becomes a stack member device, its CLI prompt changes to <stack_n.Sysname>, where n is the stack number assigned by the master device, and Sysname is its system name.

Logging in to the CLI of a member from the master

Perform this task on the master device in user view.

Task	Command
Log in to the CLI of a member device from the master device.	stack switch-to <i>member-id</i>

The **stack switch-to** command does not change the user privilege level. To return to the master device, use the **quit** command.

Displaying and maintaining stack configuration

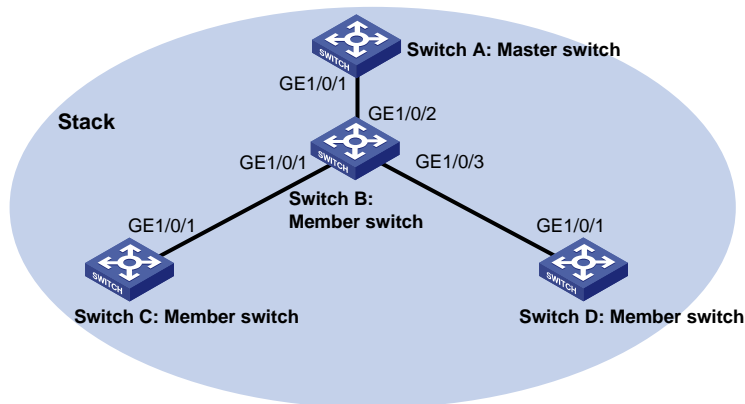
Task	Command	Remarks
Display the stack configuration of stack members.	display stack [members] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

Stack configuration example

Network requirements

Create a stack on Switch A for Switch B, Switch C, and Switch D so an administrator can access them from Switch A for easy management, as shown in [Figure 62](#).

Figure 62 Network diagram



Configuration procedure

1. Configure the master device:

Configure a private IP address pool for the stack on Switch A.

```
<SwitchA> system-view
[SwitchA] stack ip-pool 192.168.1.1 24
```

Configure GigabitEthernet 1/0/1 as a stack port on Switch A.

```
[SwitchA] stack stack-port 1 port gigabitethernet 1/0/1
```

Configure switch A as the master device.

```
[SwitchA] stack role master
```

2. Configure the member devices:

On Switch B, configure GigabitEthernet 1/0/2, GigabitEthernet 1/0/1, and GigabitEthernet 1/0/3 as stack ports.

```
<SwitchB> system-view
[SwitchB] stack stack-port 3 port gigabitethernet 1/0/1 gigabitethernet 1/0/2
gigabitethernet 1/0/3
```

On Switch C, configure GigabitEthernet 1/0/1 as a stack port.

```
<SwitchC> system-view
[SwitchC] stack stack-port 1 port gigabitethernet 1/0/1
```

On Switch D, configure GigabitEthernet 1/0/1 as a stack port.

```
<SwitchD> system-view
[SwitchD] stack stack-port 1 port gigabitethernet 1/0/1
```

3. Verify the configuration on Switch A:

```
<stack_0.SwitchA> display stack members
```

```
Number      : 0
Role        : Master
Sysname     : stack_0. SwitchA
Switch type: HP A5120-48G-PoE+ EI Switch with 2 Interface Slots
MAC address: 000f-e200-1000
```

```
Number      : 1
Role        : Slave
Sysname     : stack_1. SwitchB
Device type: HP A5120-48G-PoE+ EI Switch with 2 Interface Slots
```

MAC address: 000f-e200-1001

Number : 2

Role : Slave

Sysname : stack_2. DeviceC

Device type: HP A5120-48G-PoE+ EI Switch with 2 Interface Slots

MAC address: 000f-e200-1002

Number : 3

Role : Slave

Sysname : stack_3. DeviceD

Device type: HP A5120-48G-PoE+ EI Switch with 2 Interface Slots

MAC address: 000f-e200-1003

Support and other resources

Contacting HP

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

<http://www.hp.com/support>

Before contacting HP, collect the following information:

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

Subscription service

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

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

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

Related information

Documents

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

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

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

Websites

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

Conventions

This section describes the conventions used in this documentation set.





Command conventions

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








GUI conventions

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

Symbols

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

Network topology icons

	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the switching engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a security product, such as a firewall, a UTM, or a load-balancing or security card that is installed in a device.
	Represents a security card, such as a firewall card, a load-balancing card, or a NetStream card.

Port numbering in examples

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

Index

[A](#) [C](#) [D](#) [E](#) [F](#) [H](#) [I](#) [L](#) [M](#) [N](#) [O](#) [P](#) [R](#) [S](#) [T](#) [U](#)

A

Adding a candidate switch to a cluster, [177](#)
Alarm group configuration example, [78](#)
Applying a QoS policy, [100](#)

C

Cluster management configuration example, [181](#)
Cluster management configuration task list, [168](#)
Configuration restrictions and guidelines, [168](#)
Configuring a QoS policy, [99](#)
Configuring a schedule for an NQA test group, [125](#)
Configuring access-control rights, [19](#)
Configuring advanced cluster management functions, [177](#)
Configuring an NQA test group, [109](#)
Configuring counter sampling, [148](#)
Configuring flow sampling, [147](#)
Configuring Layer 2 remote port mirroring, [87](#)
Configuring local port mirroring, [84](#)
Configuring match criteria, [98](#)
Configuring NTP authentication, [20](#)
Configuring NTP operation modes, [14](#)
Configuring optional parameters, [17](#)
Configuring optional parameters for an NQA test group, [124](#)
Configuring PoE interface power management, [157](#)
Configuring PoE interface through PoE profile, [159](#)
Configuring SNMP basic parameters, [58](#)
Configuring SNMP logging, [63](#)
Configuring SNMP traps, [63](#)
Configuring stack ports on a member device, [186](#)
Configuring the collaboration function, [120](#)
Configuring the history records saving function, [123](#)
Configuring the management switch, [169](#)
Configuring the maximum PoE interface power, [157](#)
Configuring the member switches, [175](#)
Configuring the NQA server, [108](#)
Configuring the NQA statistics collection function, [123](#)

Configuring the PoE monitoring function, [158](#)
Configuring the RMON alarm function, [74](#)
Configuring the RMON statistics function, [73](#)
Configuring the sFlow agent and sFlow collector, [147](#)
Configuring the stack master device, [185](#)
Configuring threshold monitoring, [121](#)
Configuring traffic mirroring of different types, [99](#)
Contacting HP, [190](#)
Conventions, [191](#)
Creating an NQA test group, [109](#)

D

Detecting PDs, [156](#)
Disabling an interface from generating link up or link down logging information, [49](#)
Displaying and maintaining cluster management, [180](#)
Displaying and maintaining information center, [50](#)
Displaying and maintaining IPC, [153](#)
Displaying and maintaining NQA, [126](#)
Displaying and maintaining NTP, [21](#)
Displaying and maintaining PoE, [160](#)
Displaying and maintaining port mirroring, [92](#)
Displaying and maintaining RMON, [75](#)
Displaying and maintaining sFlow, [148](#)
Displaying and maintaining SNMP, [65](#)
Displaying and maintaining stack configuration, [187](#)
Displaying and maintaining traffic mirroring, [101](#)

E

Enabling IPC performance statistics, [152](#)
Enabling log file overwrite-protection, [50](#)
Enabling PoE for a PoE interface, [155](#)
Enabling synchronous information output, [49](#)
Enabling the NQA client, [108](#)
Ethernet statistics group configuration example, [76](#)

F

FIPS compliance, [40](#)

H

Hardware compatibility and other restrictions, [185](#)

History group configuration example, [76](#)

I

Information center configuration examples, [51](#)

Information center configuration task list, [40](#)

Introduction to port mirroring, [81](#)

Introduction to traffic mirroring, [98](#)

L

Logging in to the CLI of a member from the master, [187](#)

M

Managing security logs and the security log file, [46](#)

N

NQA configuration examples, [127](#)

NQA configuration task list, [107](#)

NTP configuration examples, [22](#)

NTP configuration task list, [14](#)

O

Outputting system information to a log host, [42](#)

Outputting system information to the console, [40](#)

Outputting system information to the log buffer, [44](#)

Outputting system information to the monitor terminal, [41](#)

Outputting system information to the SNMP module, [44](#)

Outputting system information to the trap buffer, [43](#)

Outputting system information to the Web interface, [45](#)

Overview, [154](#)

Overview, [151](#)

Overview, [71](#)

Overview, [104](#)

Overview, [9](#)

Overview, [164](#)

Overview, [34](#)

Overview, [57](#)

P

Ping, [1](#)

Ping and tracer example, [7](#)

PoE configuration example, [161](#)

PoE configuration task list, [154](#)

Port mirroring configuration examples, [92](#)

R

Related information, [190](#)

S

sFlow configuration example, [148](#)

sFlow configuration task list, [146](#)

SNMP configuration examples, [66](#)

SNMP configuration task list, [58](#)

Stack configuration example, [187](#)

Stack configuration task list, [185](#)

Switching the NM-specific interface index format, [62](#)

System debugging, [5](#)

T

Toggling between the CLIs of the management switch and a member switch, [176](#)

Tracert, [3](#)

Traffic mirroring configuration example, [101](#)

Traffic mirroring configuration task list, [98](#)

Troubleshooting PoE, [162](#)

Troubleshooting sFlow configuration, [150](#)

U

Upgrading PSE processing software in service, [160](#)