



## **CloudEngine 12800 Series Switches**

**V100R006C00**

# **NQA Technology White Paper**

**Issue 02**

**Date 2016-06-21**

**Copyright © Huawei Technologies Co., Ltd. 2016. All rights reserved.**

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

## **Trademarks and Permissions**



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

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

## **Notice**

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

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

## **Huawei Technologies Co., Ltd.**

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

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

---

# Contents

---

<b>1 Overview</b>	<b>1</b>
<b>2 Principles</b>	<b>2</b>
<b>3 Test Mechanisms</b>	<b>3</b>
3.1 ICMP Jitter Test	4
3.2 ICMP Test	4
3.3 TCP Test	5
3.4 Trace Test	5
3.5 UDP Jitter Test	6
3.6 LSP Ping Test	7
3.7 LSP Trace Test	8
<b>4 NQA Association Mechanism</b>	<b>10</b>
<b>5 Applications</b>	<b>11</b>
<b>6 Configuration Task Summary</b>	<b>13</b>
<b>7 Configuration Notes</b>	<b>14</b>
<b>8 Configuring an NQA Test Instance</b>	<b>15</b>
8.1 Configuring an ICMP Test Instance	16
8.2 Configuring an ICMP Jitter Test Instance	19
8.3 Configuring a TCP Test Instance	21
8.4 Configuring a Trace Test Instance	23
8.5 Configuring a UDP Jitter Test Instance	25
8.6 Configuring the LSP Ping Test	29
8.7 Configuring the LSP Trace Test	31
8.8 Checking the Configuration	33
<b>9 Configuring the NQA Transmission Delay Threshold and Alarm Threshold</b>	<b>34</b>
9.1 Configuring the Two-Way Transmission Delay Threshold	35
9.2 Configuring the One-Way Transmission Delay Threshold	35
<b>10 Configuring the Trap Function</b>	<b>37</b>
10.1 Enabling the NQA Alarm Function	39
10.2 Configuring the NQA Client to Send Traps When a Test Fails	39
10.3 Configuring the NQA Client to Send Traps When a Probe Fails	40

10.4 Configuring the NQA Client to Send Traps After a Probe Succeeds.....	41
10.5 Configuring the NQA Client to Send Traps When the Transmission Delay Exceeds the Threshold.....	41
10.6 Checking the Configuration.....	42
<b>11 Scheduling an NQA Test Instance.....</b>	<b>43</b>
11.1 Starting an NQA Test Instance.....	44
11.2 (Optional) Stopping an NQA Test Instance.....	45
11.3 Checking Test Results.....	46
<b>12 Maintaining NQA.....</b>	<b>48</b>
12.1 Clearing NQA Test Statistics.....	49
<b>13 Configuration Examples.....</b>	<b>50</b>
13.1 Example for Configuring an ICMP Test Instance.....	51
13.2 Example for Configuring an ICMP Jitter Test Instance.....	53
13.3 Example for Configuring a TCP Test Instance.....	55
13.4 Example for Configuring Trace Test.....	58
13.5 Example for Configuring a UDP Jitter Test Instance.....	60
13.6 Example for Configuring LSP Ping Test for LSP Tunnels.....	63
13.7 Example for Configuring LSP Trace Test for LSP Tunnels.....	67
<b>14 References.....</b>	<b>71</b>

# 1 Overview

---

## Definition

Network Quality Analysis (NQA) measures network performance and collects statistics on delay, jitter, and packet loss ratio. NQA monitors network quality of service (QoS) in real time and locates and diagnoses network faults.

## Purpose

To visualize the quality of network services and allow users to check whether the quality of network services meets requirements, the following measures must be taken:

- Collect data on network devices to describe the quality of network services.
- Deploy probe devices to monitor the quality of network services.

To carry out the preceding measures, devices must provide statistical parameters such as delay, jitter, and packet loss ratio. This requires dedicated probe devices, which increases operation costs.

NQA can precisely test the network operating status and output statistics without using dedicated probe devices, effectively reducing costs.

# 2 Principles

---

## **Constructing a test instance**

NQA requires two test ends: an NQA client and an NQA server (also called the source and destination, respectively). The NQA client initiates NQA tests, which you can configure through the command line or the network management system (NMS). NQA then places the test instances into test queues for scheduling.

## **Starting a test instance**

The user can choose to start an NQA test instance immediately, at a specified time, or after a delay. The test instance waits the specified amount of time and then generates a test packet in accordance with the test type. If the size of the test packet is smaller than the minimum size required by the protocol, the test packet is padded to the minimum size.

## **Processing a test instance**

In an NQA test instance, the operating status of the protocol is determined based on the response packets. The client adds a timestamp to the test packet according to the local system time before sending the packet to the server. After receiving the test packet, the server sends a response packet to the client. The client receives the response packet and again adds a timestamp according to the current local system time. The client then calculates the round-trip time (RTT) of the test packet based on the two timestamps.

### **NOTE**

In a jitter test instance, both the client and server add a timestamp to the sent and received packets according to the local system time. This allows the client to calculate the jitter.

You can view the test results to learn about the operating status and service quality of the network.

# 3 Test Mechanisms

---

## About This Chapter

[3.1 ICMP Jitter Test](#)

[3.2 ICMP Test](#)

[3.3 TCP Test](#)

[3.4 Trace Test](#)

[3.5 UDP Jitter Test](#)

[3.6 LSP Ping Test](#)

[3.7 LSP Trace Test](#)

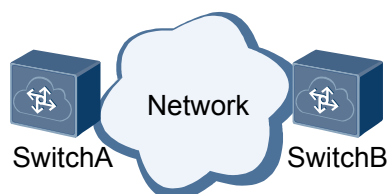
## 3.1 ICMP Jitter Test

The ICMP jitter test uses ICMP packets to determine the delay, jitter, and packet loss ratio based on the timestamps in test packets. Jitter is the interval for receiving two consecutive packets minus the interval for sending the two packets.

The ICMP jitter test process is as follows:

1. The source (SwitchA) sends packets to the destination (SwitchB) at a specified interval.
2. The destination receives the packets, adds a timestamp to them, and sends them back to the source.
3. The source receives the packets and calculates the jitter by subtracting the interval at which consecutive packets are sent from the interval at which the destination receives them.

**Figure 3-1** Network for ICMP jitter test



The following indexes are calculated based on the information received from the source:

- The maximum, minimum, and average jitter of the packets from the source to the destination and from the destination to the source.
- The maximum unidirectional delay from the source to the destination or from the destination to the source.

In an ICMP jitter test, the interval for sending packets is configurable and defaults to 20 ms. The number of packets sent each time is configurable and defaults to 60.

You can set the number of consecutive packets to be sent in a single test instance. This allows you to simulate actual data traffic for a specified period of time.

ICMP jitter test results and historical records are collected in test instances. You can run commands to view the test results and historical records.

## 3.2 ICMP Test

The NQA Internet Control Message Protocol (ICMP) test detects whether there are reachable routes from the source to the destination. It has a similar function to the ping command, but provides more output information, including:

- Average delay
- Packet loss ratio
- Time the last packet was correctly received

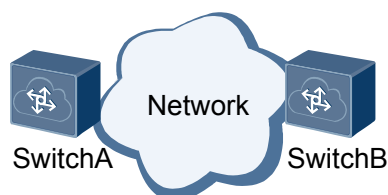
The system saves the results of the latest five tests by default.



The ICMP test process is as follows:

1. The source (SwitchA) constructs an ICMP Echo Request packet and sends it to the destination (SwitchB).
2. The destination receives the ICMP Echo Request packet and responds with an ICMP Echo Reply packet.
3. The source receives the ICMP Echo Reply packet and calculates the time between when it sent the ICMP Echo Request packet and when it received the ICMP Echo Reply packet.

**Figure 3-2** Network for ICMP test



The ICMP test results and historical records are collected in test instances. You can run commands to view the test results and historical records.

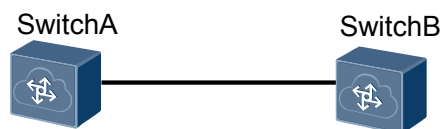
## 3.3 TCP Test

The NQA TCP test measures the time taken to set up a TCP connection between an NQA client and a TCP server through the three-way handshake.

The TCP test process is as follows:

1. The source (SwitchA) sends a TCP SYN packet to the destination (SwitchB) to set up a TCP connection.
2. The destination receives the TCP SYN packet and responds with a TCP SYN-ACK packet.
3. The source receives the SYN-ACK packet and sends an ACK packet to the destination. The connection is now established and the source can calculate the time taken.

**Figure 3-3** TCP test scenario



 **NOTE**

Frequent TCP tests can consume too many resources and affect device performance.

TCP test results and historical records are collected in test instances. You can run commands to view the test results and historical records.

## 3.4 Trace Test

The NQA trace test detects the forwarding path between the source and the destination and collects statistics about each device along the forwarding path. It has a similar function to the **tracert** command, but provides more output information, including:

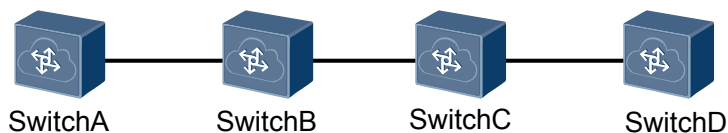
- Average delay
- Packet loss ratio
- Time of receiving the last packet

The trace test process is as follows:

1. The source (SwitchA) constructs a UDP packet, with the time-to-live (TTL) set to 1 and sends it to the destination (SwitchD).
2. When the first-hop router (SwitchB) receives the UDP packet, its TTL decreases to 0. The first-hop router discards the UDP packet and returns an ICMP Time Exceeded packet.
3. The source obtains the IP address of the first-hop router from this ICMP Time Exceeded packet. It then constructs another UDP packet with the TTL set to 2.
4. When the second-hop router (SwitchC) receives the UDP packet, its TTL decreases to 0. The second-hop router discards the UDP packet and returns an ICMP Time Exceeded packet.
5. The source continues to send UDP packets, with the TTL increasing by 1 each time. This process is repeated until the packet reaches the destination, which then returns an ICMP Port Unreachable packet to the source.

The ICMP packets from each hop give the source information about the forwarding path as well as statistics about each device along the path.

**Figure 3-4** Network for Trace test



Trace test results and historical records are collected in test instances. You can run commands to view the test results and historical records.

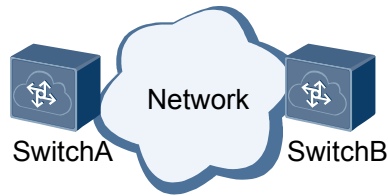
## 3.5 UDP Jitter Test

The UDP jitter test is performed using UDP packets to determine the delay, jitter, and packet loss ratio based on the timestamps in test packets. Jitter is the interval for receiving two consecutive packets minus the interval for sending the two packets.

The UDP jitter test process is as follows:

1. The source (SwitchA) sends packets to the destination (SwitchB) at a specified interval.
2. The destination receives packets, adds a timestamp to them, and sends them back to the source.
3. The source receives the returned packets and calculates the jitter by subtracting the interval at which consecutive packets were sent from the interval at which the destination received them.

**Figure 3-5** Network for UDP jitter test



The following data can be calculated based on information in the packets received by the source:

- Maximum, minimum, and average jitter of the packets from the source to the destination and from the destination to the source.
- Maximum unidirectional delay from the source to the destination or from the destination to the source.

In a UDP jitter test, the maximum number of test packets sent each time is configurable. It is the number of jitter tests (probe-count) multiplied by the number of test packets sent each time (jitter-packetnum).

You can also set the number of consecutive packets to be sent in a single test instance. This setting allows you to simulate actual traffic for a specified period of time. For example, if you set the source to send 3,000 UDP packets at an interval of 20 ms, this would simulate G.711 traffic for 1 minute.

UDP jitter test results and historical records are collected in test instances. You can run commands to view the test results and historical records.

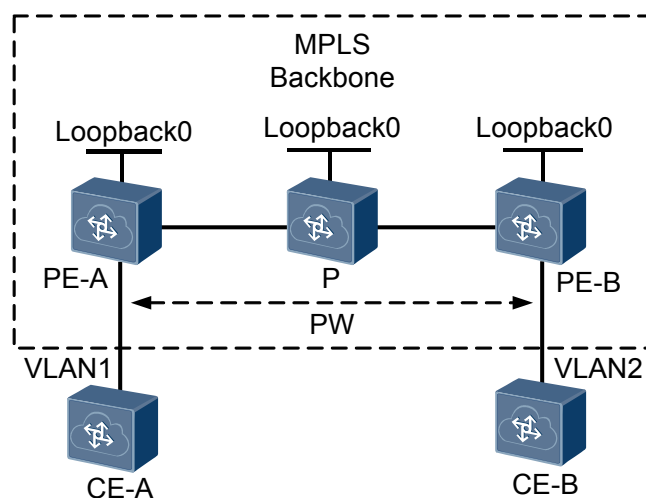
## 3.6 LSP Ping Test

The NQA label-switched paths (LSP) ping test checks the reachability of Label Distribution Protocol (LDP) LSPs.

**Figure 3-6** shows the process of an LSP ping test:

1. The source (PE-A) constructs a Multiprotocol Label Switching (MPLS) Echo Request packet whose destination IP field is an IP address on the address block 127.0.0.0/8. The source then searches for the corresponding Label Distribution Protocol (LDP) LSP based on the configured remote label switching router (LSR) ID. The source forwards the packet through that LDP LSP in the MPLS domain.
2. The destination (PE-B) egress monitors port 3503 and sends an MPLS Echo Reply packet to the source.
3. The source receives the MPLS Echo Reply packet and calculates the time taken for communication between the source and the destination.

**Figure 3-6** Network for LSP ping test



LSP ping test results and historical records are collected in test instances. You can run commands to view the test results and historical records.

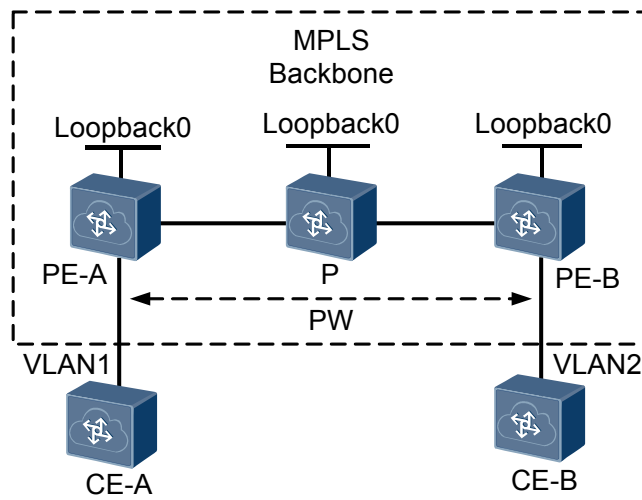
## 3.7 LSP Trace Test

The NQA LSP trace test detects the forwarding paths of LDP LSPs and collects statistics about each device along a forwarding path.

**Figure 3-7** shows the process of an LSP trace test:

1. The source (PE-A) constructs a MPLS Echo Request packet whose destination IP field is an IP address on the 127.0.0.0/8 block. The source then searches for the corresponding LSP.  
 The MPLS Echo Request packet should contain the downstream mapping type-length-value (TLV) that carries LSP downstream information on the current node, including next-hop IP address and outbound label. The TTL of the first MPLS Echo Request packet is 1.
2. The MPLS Echo Request packet is forwarded through the specified LSP in the MPLS domain. When the first hop of the LSP receives the packet, its TTL decreases to 0 and it times out. The first hop then returns an MPLS Echo Reply packet.
3. The source continues to send MPLS Echo Request packets, with the TTL increasing by 1 each time. This process is repeated until all the LSRs along the LSP have returned their responses.
4. According to the MPLS Echo Reply packet received from each hop, the source obtains the LSP forwarding path from the source to the destination and collects statistics about each device along the forwarding path.

**Figure 3-7** Network for LSP trace test



The LSP trace test results and historical records are collected in test instances. You can run commands to view the test results and historical records.

# 4 NQA Association Mechanism

---

NQA provides test results for other modules so that other modules can take measures according to test results. Currently, NQA can be associated with the Virtual Router Redundancy Protocol (VRRP), static routes, and policy-based routing (PBR).

The following uses a static route as an example.

In this example, there is a static route with next hop 192.168.0.88. Association between the NQA module and application module determines the validity of the static route in real time. If the NQA module finds that next hop 192.168.0.88 is unreachable, it notifies the static route module. The static route module then determines whether the static route is invalid.

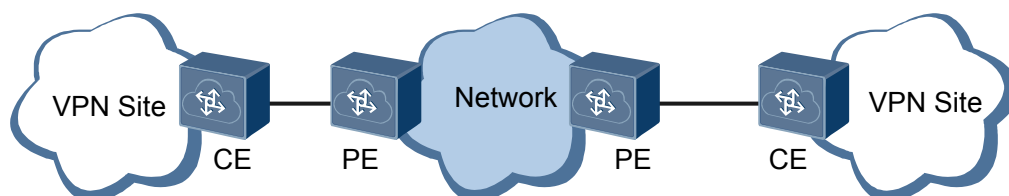
# 5 Applications

## Performing Network Diagnosis

Networks often encounter such problems as intermittent network disconnections, failure to access websites, slow Internet access, and slow file downloading. When these occur, you can locate the fault by collecting statistics about network devices. These statistics must be provided by the devices.

In the example shown in [Figure 5-1](#), users in different places connect to each other over a VPN. They find, for instance, that the network intermittently disconnects and the connection is slow.

**Figure 5-1** Performing network diagnosis

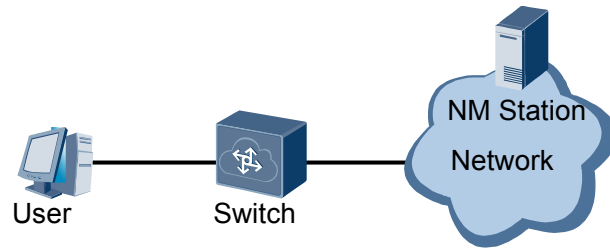


In this situation, you can deploy NQA on PEs to analyze network quality. Perform an ICMP test between the PEs and CEs to check the continuity of the network. After confirming that the network is correctly connected, perform a jitter test to measure network jitter. Then perform the same tests between the PEs. Analyze the test data and the faults that users encounter to locate the source of these faults.

## Learning About Network Service Quality

In [Figure 5-2](#), you can perform an NQA test on a switch to obtain statistics about the network operating status. This provides information about network service quality.

**Figure 5-2** Learning about network service quality





# 6 Configuration Task Summary

---

## Configuring Basic NQA Test Functions

You can perform an NQA test by [8 Configuring an NQA Test Instance](#) and [11 Scheduling an NQA Test Instance](#).

## Configuring Extended NQA Test Functions

The following extended NQA functions are optional in NQA configuration:

- [9 Configuring the NQA Transmission Delay Threshold and Alarm Threshold](#)
- [10 Configuring the Trap Function](#)

# 7 Configuration Notes

This section provides the points of attention when configuring NQA.

## Involved Network Elements

Other network elements are not required.

## License Support

The NQA IPv6 function is controlled by a license. By default, this function is disabled on new purchased CE12800 series switches. To use the NQA IPv6 feature, apply for and purchase the license from the equipment supplier.

## Version Support

**Table 7-1** Products and minimum version supporting NQA

Series	Product	Minimum Version Required
CE12800	CE12804/CE12808/ CE12812	V100R001C00
	CE12816	V100R003C00
	CE12804S/CE12808S	V100R005C00

## Feature Dependencies and Limitations

- The type of a running test instance cannot be changed. If you change the type of a running NQA test instance, the test instance will fail.
- If the number of running test instances reaches the maximum value defined by the system, the **start** command is invalid.

# 8 Configuring an NQA Test Instance

---

## About This Chapter

You can configure an NQA test instance to perform an NQA test of a specified type.

### Pre-configuration Tasks

Before configuring the NQA test instance, complete the following tasks:

- Ensure that the device is running properly.
- Configure routing to ensure reachable routes between devices involved in the test.

 **NOTE**

The pre-configuration tasks differ from different test instances. For details, see the configuration of each test instance.

### Configuration Process

The following optional test instances are independent of each other:

[8.1 Configuring an ICMP Test Instance](#)

[8.2 Configuring an ICMP Jitter Test Instance](#)

[8.3 Configuring a TCP Test Instance](#)

[8.4 Configuring a Trace Test Instance](#)

[8.5 Configuring a UDP Jitter Test Instance](#)

[8.6 Configuring the LSP Ping Test](#)

[8.7 Configuring the LSP Trace Test](#)

[8.8 Checking the Configuration](#)

## 8.1 Configuring an ICMP Test Instance

### Context

Before configuring an ICMP test instance, configure reachable routes between the NQA client and the tested device.

An ICMP test has the same function as the **ping** command but displays more detailed information.

#### NOTE

Perform the following steps on the NQA client.

The **timeout**, **probe-count**, **frequency**, and **interval** commands constrain each other; therefore, properly set the values when running the four commands. Improper command settings may lead to test failure.

- On a network with poor quality and low transmission rate, increase the **timeout** value to ensure that the response to NQA detection packets can be received.
- On a network with low reliability, increase the **probe-count** value because multiple detection packets may need to be sent to ensure successful detection.
- The **interval** value must be larger than the **timeout** value.
- The **frequency** value must comply with the following rules:

$$\text{frequency} > \text{interval} \times (\text{probe-count} - 1) + \text{timeout}$$

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
nqa test-instance admin-name test-name
```

An NQA test instance is created, and the NQA view is displayed.

By default, no NQA test instance is created.

#### Step 3 Run:

```
test-type icmp
```

The test type is set to ICMP.

By default, no test type is configured.

#### Step 4 Run:

```
destination-address { ipv4 ipv4-address | ipv6 ipv6-address }
```

The destination address is configured.

By default, destination address is not configured for an NQA test instance.

#### Step 5 (Optional) Run the following commands as required to configure parameters for the ICMP test.

- Run:

```
description string
```

A description is configured for the test instance.

By default, no description is configured for an NQA test instance.

- Run:

```
frequency interval
```

The interval at which the NQA test instance is automatically executed is set.

By default, the interval at which an NQA test instance is automatically performed is not configured. That is, the test is performed for one time.

- Run:

```
timeout time
```

The timeout period of a probe is set for the NQA test instance.

By default, the timeout period of an ICMP probe is 3 seconds.

- Run:

```
source-interface interface-type interface-number
```

The source interface that sends test packets is configured.

By default, no source interface is configured for an NQA test instance.

- Run:

```
source-address { ipv4 ipv4-address | ipv6 ipv6-address }
```

The source IP address is configured.

*ip-address* and *ipv6-address* are similar to **-a** in the **ping** command.

By default, the IP address of the interface where packets are sent functions as the source IP address of a test instance.

- Run:

```
ttl number
```

The TTL value is set.

*number* is similar to **-h** in the **ping** command.

The default TTL value is 30.

- Run:

```
datasize size
```

The size of Echo Request packets excluding the IP header is configured.

*size* is similar to **-s** in the **ping** command.

The default size is 0, which indicates that the test packet does not carry data information.

- Run:

```
datafill fillstring
```

The padding field is configured.

*fillstring* is similar to **-p** in the **ping** command.

By default, there are no padding characters in an NQA test instance.

- Run:

```
sendpacket passroute
```

The NQA test instance is configured to send packets without searching the routing table.

By default, the test packet is sent according to the routing table.

- Run:

```
probe-count number
```

The number of probes in a test is set.

By default, the number of probes for an NQA test instance is 3.

- Run:

```
tos value
```

The type of service (ToS) field value in an IP header is configured.

*value* is similar to **-tos** in the **ping** command.

By default, the ToS value is 0.

- Run:

```
fail-percent percent
```

The failure percentage is set for the NQA test instance.

By default, the failure percentage is 100%. That is, the test is regarded as a failure only when all the probes fail.

- Run:

```
interval seconds interval
```

The interval at which test packets are sent is configured.

*interval* is similar to **-m** in the **ping** command.

By default, The interval is 4 seconds for ICMP test instance.

- Run:

```
vpn-instance vpn-instance-name
```

The VPN instance name is configured.

By default, no VPN instance is configured.

- Run:

```
records history number
```

The maximum number of historical records is set for the NQA test instance.

By default, the number of history records is 50.

- Run:

```
records result number
```

The maximum number of result records is set for the NQA test instance.

By default, the number of test results is 5.

- Run:

```
agetime hh:mm:ss
```

The aging time is set for the NQA test instance.

The default aging time of an NQA test instance is 0, indicating that the test instance is not aged.

**Step 6** Run:

```
commit
```

The configuration is committed.

----End

## 8.2 Configuring an ICMP Jitter Test Instance

### Context

Before configuring an ICMP jitter test, ensure that the NQA client and the tested device have reachable routes to each other.

When configuring an ICMP jitter test instance, you can set the number of packets to be sent consecutively in a single test. This configuration can simulate traffic of various types in a specified period. For example, you can simulate voice service traffic through this configuration.

#### NOTE

Perform the following steps on the NQA client. The NQA client also functions as the ICMP jitter client.

The **timeout**, **probe-count**, **frequency**, **jitter-packetnum**, and **interval** commands constrain each other; therefore, properly set the values when running the five commands. Improper command settings may lead to test failure.

- On a network with poor quality and low transmission rate, increase the **timeout** value to ensure that the response to NQA detection packets can be received.
- On a network with low reliability, increase the **probe-count** value because multiple detection packets may need to be sent to ensure successful detection.
- The **frequency** value must comply with the following rules:

$$\text{frequency} > \text{interval} \times (\text{probe-count} \times \text{jitter-packetnum} - 1) + \text{timeout}$$

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
nqa test-instance admin-name test-name
```

An NQA test instance is created, and the NQA view is displayed.

#### Step 3 Run:

```
test-type icmpjitter
```

The test type is set to ICMP Jitter.

#### Step 4 Run:

```
destination-address ipv4 ipv4-address
```

The destination address is configured.

#### Step 5 Configure global parameters for the test instance to simulate network packets.

- Run:

```
description string
```

A description is configured for the test instance.

- Run:

```
frequency interval
```

- The test period is set for the NQA test instance.  
Run:  
`timeout time`  
The timeout period of a probe is set for the NQA test instance.
- Run:  
`fail-percent percent`  
The failure percentage is set for the NQA test instance.  
By default, the failure percentage is 100%, that is, the test is regarded failed only when all the probes fail.
- Run:  
`icmp-jitter-mode { icmp-echo | icmp-timestamp }`  
An NQA ICMP jitter test instance is created.
- Run:  
`datafill fillstring`  
The padding field is configured.
- Run:  
`datasize size`  
The size of Echo Request packets without the IP header is configured.
- Run:  
`jitter-packetnum number`  
The number of packets sent each time in a probe is set.
- Run:  
`probe-count number`  
The number of probes in a test is set.
- Run:  
`interval { milliseconds interval | seconds interval }`  
The interval at which NQA test packets are sent is set.  
A shorter interval enables a test to be complete sooner. Delays occur during the sending and receiving of test packets on the processor. Therefore, if the interval for sending test packets is short, the ICMP Jitter test results are inaccurate.
- Run:  
`source-interface interface-type interface-number`  
The source interface used to send test packets is configured.
- Run:  
`source-address ipv4 ipv4-address`  
The source IP address is set.
- Run:  
`ttl number`  
The TTL value in the NQA test packet is set.
- Run:  
`tos value`  
Type of Service (ToS) is set for the test packet.
- Run:  
`vpn-instance vpn-instance-name`



The VPN instance name is configured.

- Run:

```
records history number
```

The maximum number of historical records is set for the NQA test instance.

- Run:

```
records result number
```

The maximum number of result records is set for the NQA test instance.

- Run:

```
agetime hh:mm:ss
```

The aging time is set for the NQA test instance.

#### Step 6 Run:

```
commit
```

The configuration is committed.

---End

## 8.3 Configuring a TCP Test Instance

### Context

Before configuring a TCP test instance, configure a TCP server and ensure reachable routes between the TCP client and the TCP server.

An NQA TCP test measures the speed at which a TCP connection can be set up between an NQA client and a TCP server through the three-way handshake.

#### NOTE

The NQA client also functions as the TCP client.

The **timeout**, **probe-count**, **frequency**, and **interval** commands constrain each other; therefore, properly set the values when running the four commands. Improper command settings may lead to test failure.

- On a network with poor quality and low transmission rate, increase the **timeout** value to ensure that the response to NQA detection packets can be received.
- On a network with low reliability, increase the **probe-count** value because multiple detection packets may need to be sent to ensure successful detection.
- The **interval** value must be larger than the **timeout** value.
- The **frequency** value must comply with the following rules:  
**frequency > interval x (probe-count - 1) + timeout**

### Procedure

- Configure the TCP server.

- a. Run:

```
system-view
```

The system view is displayed.

- b. Run:

```
nqa server tcpconnect [ vpn-instance vpn-instance-name ] ip-address port-number
```

- The monitoring IP address and port number of the TCP server are configured.
- Configure the NQA client.
    - a. Run:  

```
system-view
```

The system view is displayed.
    - b. Run:  

```
nqa test-instance admin-name test-name
```

An NQA test instance is created, and the NQA view is displayed.
    - c. Run:  

```
test-type tcp
```

The test type is set to TCP.
    - d. Run:  

```
destination-address ipv4 ipv4-address
```

The destination IP address is configured.
    - e. (Optional) Run the following commands as required to configure parameters for the TCP test.
      - Run:  

```
description string
```

A description is configured for the test instance.
      - Run:  

```
frequency interval
```

The test period is set for the NQA test instance.
      - Run:  

```
timeout time
```

The timeout period of a probe is set for the NQA test instance.
      - Run:  

```
destination-port port-number
```

The destination port number is configured.
      - Run:  

```
source-address ipv4 ipv4-address
```

The source IP address is configured.
      - Run:  

```
source-port port-number
```

The source port number is configured.
      - Run:  

```
ttl number
```

The TTL value in the NQA test packet is set.
      - Run:  

```
sendpacket passroute
```

The NQA test instance is configured to send packets without searching the routing table.
      - Run:  

```
probe-count number
```

- The number of probes in a test is set.  
Run:  
`tos value`  
Type of Service (TOS) is set for the test packet.
  - Run:  
`fail-percent percent`  
The failure percentage is set for the NQA test instance.
  - Run:  
`interval seconds interval`  
The interval at which test packets are sent is configured.
  - Run:  
`vpn-instance vpn-instance-name`  
The VPN instance name is configured.
  - Run:  
`records history number`  
The maximum number of historical records is set for the NQA test instance.
  - Run:  
`records result number`  
The maximum number of result records is set for the NQA test instance.
  - Run:  
`agetime hh:mm:ss`  
The aging time is set for the NQA test instance.
- f. Run:  
`commit`  
The configuration is committed.

----End

## 8.4 Configuring a Trace Test Instance

### Context

An NQA trace test detects the forwarding path between the source and the destination and collects statistics, such as delay, about each device along the forwarding path. The function of a trace test is similar to the function of the **tracert** command, except that the trace test provides more information. Information about each hop includes the average delay, packet loss ratio, and time of receiving the last packet.

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
nqa test-instance admin-name test-name
```

An NQA test instance is created, and the NQA view is displayed.

**Step 3** Run:

```
test-type trace
```

The test type is set to trace.

**Step 4** Run:

```
destination-address { ipv4 ipv4-address | ipv6 ipv6-address }
```

The destination address for the trace instance test is configured.

**Step 5** (Optional) Run the following commands as required to configure parameters for the trace test instance.

- Run:

```
description string
```

A description is configured for the test instance.

- Run:

```
destination-port port-number
```

The destination port number is configured.

- Run:

```
source-address { ipv4 ipv4-address | ipv6 ipv6-address }
```

The source IP address is configured.

- Run:

```
tracert-lifetime first-ttl first-ttl max-ttl max-ttl
```

The initial and the maximum TTL of the packet are configured.

- Run:

```
tracert-hopfailtimes times
```

The hop fail times are set.

- Run:

```
set-df
```

Packet fragmentation is prohibited.

 **NOTE**

This command is invalid when the source and destination addresses are IPv6 addresses.

- Run:

```
datasize size
```

The packet size is set.

- Run:

```
datafill fillstring
```

The padding field is configured.

- Run:



```
sendpacket passroute
```

The NQA test instance is configured to send packets without searching the routing table.

- Run:

```
vpn-instance vpn-instance-name
```

The VPN instance name is configured.

- Run:  
`records history number`  
The maximum number of historical records is set.
- Run:  
`records result number`  
The maximum number of result records is set.
- Run:  
`agetime hh:mm:ss`  
The aging time is set for the test instance.
- Run:  
`timeout time`  
The timeout period of a probe is set.
- Run:  
`probe-count number`  
The number of probes in a test is set.  
 **NOTE**  
When a trace test instance is used, the number of probes for each test cannot be larger than 10.
- Run:  
`frequency interval`  
The test period is set.  
 **NOTE**
  - When a trace test instance is used, the test period cannot be shorter than 60s.
  - The **timeout**, **probe-count**, and **frequency** commands constrain each other; therefore, properly set the values when running the three commands. Improper command settings may lead to test failure.
    - On a network with poor quality and low transmission rate, increase the **timeout** value to ensure that the response to NQA detection packets can be received.
    - On a network with low reliability, increase the **probe-count** value because multiple detection packets may need to be sent to ensure successful detection.

**Step 6** Run:

```
commit
```

The configuration is committed.

----End

## 8.5 Configuring a UDP Jitter Test Instance

### Context

When configuring a UDP Jitter test instance, configure reachable routes between the UDP Jitter client and the UDP Jitter server.

You can set the number of packets to be sent consecutively in each test instance. This configuration is used to simulate certain traffic. For example, G.711 traffic can be simulated within 1 minute by sending 3000 UDP packets at an interval of 20 milliseconds.

 **NOTE**

Configuring NTP on the client and the server can effectively improve the accuracy of the test.

The NQA client also functions as the UDP Jitter client. The jitter obtained in this test is the UDP Jitter. Perform the following steps on the NQA client.

The **timeout**, **probe-count**, **frequency**, **jitter-packetnum**, and **interval** commands constrain each other; therefore, properly set the values when running the five commands. Improper command settings may lead to test failure.

- On a network with poor quality and low transmission rate, increase the **timeout** value to ensure that the response to NQA detection packets can be received.
- On a network with low reliability, increase the **probe-count** value because multiple detection packets may need to be sent to ensure successful detection.
- The **frequency** value must comply with the following rules:

$$\text{frequency} > \text{interval} \times (\text{probe-count} \times \text{jitter-packetnum} - 1) + \text{timeout}$$

## Procedure

- Configure the UDP Jitter server.

- a. Run:

```
system-view
```

The system view is displayed.

- b. Run:

```
nqa server udpecho [ vpn-instance vpn-instance-name ] ip-address port-number
```

The monitoring IP address and port number of the UDP server are configured.

- Configure the NQA client.

- a. Run:

```
system-view
```

The system view is displayed.

- b. (Optional) Run:

```
nqa jitter tag-version version-number
```

The version number is configured for Jitter packets.

By default, the version number of Jitter test packets is 1.

After setting the version number of the Jitter test packets to 2 and enabling the NQA client to collect statistics about packet loss in one direction, you can view the number of lost packets on the link from the source to the destination, from the destination to the source, or from unknown directions. Based on these statistics, you can easily locate network faults and detect malicious attacks.

- c. Run:

```
nqa test-instance admin-name test-name
```

An NQA test instance is created, and the NQA view is displayed.

- d. Run:

```
test-type jitter
```

The test type is set to Jitter.

- e. Run:

```
destination-address ipv4 ipv4-address
```

The destination address is configured.

f. Run:

```
destination-port port-number
```

The destination port number is configured.

g. (Optional) Run the following commands as required to configure parameters for the Jitter test:

■ Run:

```
description string
```

A description is configured for the test instance.

■ Run:

```
frequency interval
```

The test period is set for the NQA test instance.

■ Run:

```
timeout time
```

The timeout period of a probe is set for the NQA test instance.

■ Run:

```
source-address { ipv4 ipv4-address | ipv6 ipv6-address }
```

The source IP address is configured.

■ Run:

```
source-interface interface-type interface-number
```

The source interface used to send test packets is configured.

■ Run:

```
source-port port-number
```

The source port number is configured.

■ Run:

```
ttl number
```

The TTL value in the NQA test packet is set.

■ Run:

```
datasize size
```

The packet size is set for the NQA test instance.

■ Run:

```
datafill fillstring
```

The padding field is configured for the NQA test instance.

■ Run:

```
sendpacket passroute
```

The NQA test instance is configured to send packets without searching the routing table.

By default, the NQA test packets are sent with searching the routing table.

■ Run:

```
probe-count number
```

The number of probes in each test is set.

By default, the number of probes is 3.

■ Run:

**tos value**

Type of Service (TOS) is set for the test packet.

- Run:

**fail-percent percent**

The failure percentage is set for the NQA test instance.

By default, the failure percentage is 100%, that is, the test is regarded failed only when all the probes fail.

- Run:

**interval { milliseconds interval | seconds interval }**

The interval at which test packets are sent is set.

A shorter interval enables a test to be complete sooner. Delays occur during the sending and receiving of test packets on the processor. Therefore, if the interval for sending test packets is short, the Jitter test results are inaccurate.

- Run:

**jitter-packetnum number**

The number of test packets sent in each probe is set.

By default, 20 packets are sent each time in each test.

The Jitter test is used to collect and analyze the delay variation during the UDP packet transmission. To improve the accuracy of the test result, the system sends multiple test packets each time. The more test packets are sent, the more accurate the statistics are, and the longer the test lasts.

 **NOTE**

The **probe-count** command sets the number of Jitter probes and the **jitter-packetnum** command sets the number of test packets sent during each probe. The product of probe count multiplied by the number of test packets must be smaller than or equal to 3000.

- Run:

**jitter-codec { g711a | g711u | g729a }**

The code type is configured for jitter tests of analog voice services.

This command is applied only to jitter tests of analog voice services.

- Run:

**adv-factor factor-value**

The advantage factor is configured for analog voice test calculation.

This command is applied only to jitter tests of analog voice services.

- Run:

**vpn-instance vpn-instance-name**

The VPN instance name is configured.

- Run:

**records history number**

The maximum number of historical records is set for the NQA test instance.

- Run:

**records result number**

The maximum number of result records is set for the NQA test instance.

- Run:

**agetime hh:mm:ss**

The aging time is set for the NQA test instance.



h. Run:

```
commit
```

The configuration is committed.

----End

## 8.6 Configuring the LSP Ping Test

### Context

The NQA LSP Ping test can be used to test the reachability of the LSP tunnel.

#### NOTE

Perform the following steps on the NQA client.

The **timeout**, **probe-count**, **frequency**, and **interval** commands constrain each other; therefore, properly set the values when running the four commands. Improper command settings may lead to test failure.

- On a network with poor quality and low transmission rate, increase the **timeout** value to ensure that the response to NQA detection packets can be received.
- On a network with low reliability, increase the **probe-count** value because multiple detection packets may need to be sent to ensure successful detection.
- The **interval** value must be larger than the **timeout** value.
- The **frequency** value must comply with the following rules:  
**frequency** > **interval** x (**probe-count** - 1) + **timeout**

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
nqa test-instance admin-name test-name
```

An NQA test instance is created and the test instance view is displayed.

**Step 3** Run:

```
test-type lsping
```

The test type is set to LSP ping.

**Step 4** Configure the LSP ping test for the LSP tunnel.

- Run:

```
lsp-type ipv4
```

The test type of the LSP Ping is configured.

- Run:

```
destination-address ipv4 ipv4-address [ lsp-masklen masklen | lsp-loopback  
loopback-address ] *
```

The destination IP address to be tested is configured.


**Step 5** (Optional) Perform the following as required to configure other parameters for the LSP ping test:

- Run:  

```
lsp-nexthop nexthop-ip-address
```

The next-hop IP address in the scenario where load balancing is enabled is configured on the initiator of the LSP ping test.
- Run:  

```
lsp-replymode { level-control-channel | no-reply | udp }
```

The response mode of the LSP Ping test is set.  
 **NOTE**

In a uni-directional LSP Ping test, if the **lsp-replymode no-reply** command is configured, the test result displays that the test fails regardless of whether the test is successful or fails. If the test is successful, the test result also displays the number of the timeout packets. If the test fails, the test result displays the number of the discarded packets.
- Run:  

```
lsp-exp exp
```

The LSP EXP value is set.
- Run:  

```
description string
```

A description is configured for the test instance.
- Run:  

```
frequency interval
```

The test period is set.
- Run:  

```
timeout time
```

The timeout period of a probe is set.
- Run:  

```
source-address ipv4 ipv4-address
```

The source IP address is configured.
- Run:  

```
ttl number
```

The TTL value is set.
- Run:  

```
datafill fillstring
```

The padding field is configured.
- Run:  

```
datasize size
```

The packet size is set.
- Run:  

```
probe-count number
```

The number of probes in each test is set.  
By default, the number of probes is 3.
- Run:  

```
fail-percent percent
```

The failure percentage is set.  
By default, the failure percentage is 100%, that is, the test is regarded failed only when all the probes fail.

- Run:  
`interval seconds interval`  
The interval at which test packets are sent is set.  
By default, test packets are sent at an interval of 4 seconds.
- Run:  
`records history number`  
The maximum number of historical records is set.
- Run:  
`records result number`  
The maximum number of result records is set.
- Run:  
`agetime hh:mm:ss`  
The aging time is set for the test instance.

**Step 6** Run:

```
commit
```

The configuration is committed.

----End

## 8.7 Configuring the LSP Trace Test

### Context

The NQA LSP Trace test can be used to test the invalid nodes on the LSP tunnel.

 **NOTE**

Perform the following steps on the NQA client.

The **timeout**, **probe-count**, and **frequency** commands constrain each other; therefore, properly set the values when running the three commands. Improper command settings may lead to test failure.

- On a network with poor quality and low transmission rate, increase the **timeout** value to ensure that the response to NQA detection packets can be received.
- On a network with low reliability, increase the **probe-count** value because multiple detection packets may need to be sent to ensure successful detection.
- The **frequency** value must be larger than or equal to 60s.

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
nqa test-instance admin-name test-name
```

An NQA test instance is created and the test instance view is displayed.

**Step 3** Run:

```
test-type lsptrace
```

The test type is set to LSP Trace.

**Step 4** Configure the LSP trace test for the LSP tunnel.

- Run:

```
lsp-type ipv4
```

The test type of LSP Trace is configured.

- Run:

```
destination-address ipv4 ipv4-address [ lsp-masklen masklen | lsp-loopback  
loopback-address ] *
```

The destination IP address to be tested is configured.

**Step 5** (Optional) Perform the following as required to configure other parameters for the LSP Trace test:

- Run:

```
lsp-replymode { level-control-channel | no-reply | udp }
```

The response mode of the LSP trace test is set.

 **NOTE**

In a uni-directional LSP Trace test, if the **lsp-replymode no-reply** command is configured, the test result displays that the test fails regardless of whether the test is successful or fails. If the test is successful, the test result also displays the number of the timeout packets. If the test fails, the test result displays the number of the discarded packets.

- Run:

```
lsp-exp exp
```

The LSP EXP value is set.

- Run:

```
tracert-hopfailtimes times
```

The number of hops after which the test is considered failed is set.

- Run:

```
tracert-livetime first-ttl first-ttl max-ttl max-ttl
```

The initial and the maximum TTL values of the packet are set.

- Run:

```
description string
```

A description is configured for the test instance.

- Run:

```
frequency interval
```

The test period is set.

- Run:

```
timeout time
```

The timeout period of a probe is set.

- Run:

```
source-address ipv4 ipv4-address
```

The source IP address is configured.

- Run:

```
probe-count number
```

The number of probes in each test is set.

By default, the number of probes is 3.

- Run:

```
records history number
```

The maximum number of historical records is set.

- Run:

```
records result number
```

The maximum number of result records is set.

- Run:

```
agetime hh:mm:ss
```

The aging time is set for the test instance.

#### Step 6 Run:

```
commit
```

The configuration is committed.

---End

## 8.8 Checking the Configuration

### Prerequisites

After completing NQA configuration, run the following commands to check the NQA configuration.

### Procedure

- Run the **display nqa server** command on the NQA server to check information about the server.

---End

# 9 Configuring the NQA Transmission Delay Threshold and Alarm Threshold

---

## About This Chapter

The statistics about the test packets that exceed the threshold are displayed in the NQA test result. This provides a basis for the network administrators to analyze the operating status of the specified service. The alarm information is sent to the NMS to report the change to the device.

### Pre-configuration Tasks

Before configuring the NQA transmission threshold and alarm function, complete the following tasks:

- Ensure that the device is running properly.
- Create the NQA test instance and configuring related parameters.

### Configuration Process

The configured NQA transmission threshold and alarm threshold help you obtain the statistics about the test packet that exceed the thresholds in the test result. This improves the NQA function and provides an optional configuration for NQA test.

The alarm information can be sent to the NMS only when the routes between the device and NMS are reachable and the related configurations are completed.

#### NOTE

For the ICMP Jitter, LSP ping, and LSP Trace test instances, the trap sending conditions cannot be configured.

Perform the following configurations on the NQA client:

[9.1 Configuring the Two-Way Transmission Delay Threshold](#)

[9.2 Configuring the One-Way Transmission Delay Threshold](#)

## 9.1 Configuring the Two-Way Transmission Delay Threshold

### Context

If the two-way transmission delay threshold is configured for an NQA test instance, the statistics about the test packets that exceed the threshold are displayed in the test result. This provides a basis for the network administrators to analyze the operating status of the specified service.

#### NOTE

The one-way transmission delay threshold can be configured only when the **test-type** is set to **trace**, **icmp**, **jitter**, and **tcp**.

This two-way transmission delay refers to the round-trip transmission delay.

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
nqa test-instance admin-name test-name
```

The NQA view is displayed.

#### Step 3 Run:

```
threshold rtd rtd-value
```

The two-way transmission delay threshold is configured.

By default, no two-way transmission delay threshold is configured.

#### Step 4 Run:

```
commit
```

The configuration is committed.

----End

## 9.2 Configuring the One-Way Transmission Delay Threshold

### Context

In Jitter tests, after the one-way transmission delay threshold is configured, the test results show statistics about the test packets of which the transmission exceeds the threshold. Network administrators can analyze the operating status of the network according to the test results.

 **NOTE**

The one-way transmission delay threshold can be configured only when the **test-type** is set to **jitter**.  
You can perform either of [Step 3](#) and [Step 4](#) or both of them in any sequence.

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
nqa test-instance admin-name test-name
```

The NQA view is displayed.

**Step 3** Run:

```
threshold owd-sd owd-sd-value
```

The one-way transmission delay threshold (from the source to the destination) is configured.

By default, no one-way transmission delay threshold is configured.

**Step 4** Run:

```
threshold owd-ds owd-ds-value
```

The one-way transmission delay threshold (from the destination to the source) is configured.

By default, no one-way transmission threshold is configured.

**Step 5** Run:

```
commit
```

The configuration is committed.

----End



# 10 Configuring the Trap Function

---

## About This Chapter

### Context

A device generates traps no matter whether a NQA test succeeds or fails. NQA supports three types of traps as defined in DISMAN-PING-MIB. NQA also supports the sending of traps to the NMS when the one-way or two-way transmission delay exceeds the threshold.

- For some test instances, if the two-way transmission delay exceeds the threshold and the trap function is enabled, traps are sent to the NMS with the specified IP address.
- During a jitter test, if the one-way delay from the source to the destination or from the destination to the source exceeds the threshold and the trap function is enabled, the NQA client sends a trap message to the specified NMS IP address.

Traps carry the following information: destination IP addresses, operating status, destination IP address of the test packet, minimum RTT, maximum RTT, total RTT, number of sent probe packets, number of received packets, RTT square sum, and time of the latest successful probe.

### Pre-configuration Tasks

Before configuring the trap function of the NQA test, complete the following tasks:

- Configure reachable routes between the NQA client and the NMS.
- Create the NQA test instance and configure related parameters.

### Configuration Process

The following optional configuration tasks are performed on the NQA client.

These configurations take effect only after the NQA alarm function is enabled.

#### NOTE

For the ICMP Jitter, LSP ping, and LSP Trace test instances, the trap sending conditions cannot be configured.

#### [10.1 Enabling the NQA Alarm Function](#)

[10.2 Configuring the NQA Client to Send Traps When a Test Fails](#)

[10.3 Configuring the NQA Client to Send Traps When a Probe Fails](#)

[10.4 Configuring the NQA Client to Send Traps After a Probe Succeeds](#)

[10.5 Configuring the NQA Client to Send Traps When the Transmission Delay Exceeds the Threshold](#)

[10.6 Checking the Configuration](#)

## 10.1 Enabling the NQA Alarm Function

### Context

After the NQA alarm function is enabled, the device sends alarms to the NMS.

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
snmp-agent trap enable feature-name nqa [ trap-name  
{ nqajitterstatsowdthresholdnotificationds |  
nqajitterstatsowdthresholdnotificationds | nqajitterstatsrtdthresholdnotification  
| nqajitterstatstestfailed | nqaresultsprobefailed | nqaresultstestcompleted |  
nqaresultstestfailed | nqaresultsthresholdnotification | pingprobefailed |  
pingtestcompleted | pingtestfailed | traceroutetestcompleted |  
traceroutetestfailed | nqajitterstatsprobefailed | nqajitterstatstestcompleted |  
hwlsptimeprobe | hwlsppingprobe } ]
```

The alarm function is enabled for the NQA module.

By default, the alarm function is enabled for the NQA module.

**Step 3** Run:

```
commit
```

The configuration is committed.

----End

## 10.2 Configuring the NQA Client to Send Traps When a Test Fails

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
nqa test-instance admin-name test-name
```

The NQA view is displayed.

**Step 3** Run:

```
send-trap testfailure
```

The NQA client is configured to send traps when the test fails.

By default, the NQA client sends no trap when an NQA test fails.

**Step 4** Run:

```
test-failtimes times
```

The threshold on the traps sent after the NQA test fails is configured, The threshold specifies maximum number of continuous test failures for the NQA test instance.

By default, a trap is sent for each test failure.

**Step 5** Run:

```
commit
```

The configuration is committed.

---End

## 10.3 Configuring the NQA Client to Send Traps When a Probe Fails

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
nqa test-instance admin-name test-name
```

The NQA view is displayed.

**Step 3** Run:

```
send-trap probefailure
```

The NQA client is configured to send traps when a probe fails.

By default, the NQA client sends no trap when a probe fails.

#### NOTE

This command cannot be configured when the **test-type** is set to **jitter** and **trace**.

**Step 4** Run:

```
probe-failtimes times
```

The threshold on the traps sent after the probe fails is configured, The threshold specifies maximum number of continuous probe failures for the NQA test instance.

By default, a trap is sent for each probe failure.

#### NOTE

This command cannot be configured when the **test-type** is set to **jitter** and **trace**.

**Step 5** Run:

```
commit
```

The configuration is committed.

----End

## 10.4 Configuring the NQA Client to Send Traps After a Probe Succeeds

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
nqa test-instance admin-name test-name
```

The NQA view is displayed.

**Step 3** Run:

```
send-trap testcomplete
```

The NQA client is configured to send traps when a probe succeeds.

By default, the NQA client sends no trap when a probe succeeds.

 **NOTE**

This command cannot be configured when the **test-type** is set to **jitter**.

**Step 4** Run:

```
commit
```

The configuration is committed.

----End

## 10.5 Configuring the NQA Client to Send Traps When the Transmission Delay Exceeds the Threshold

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
nqa test-instance admin-name test-name
```

The NQA view is displayed.

**Step 3** Run:

```
send-trap { owd-ds | owd-sd | rtd }*
```

The NQA client is configured to send traps when the transmission delay exceeds the threshold.

By default, the NQA client sends no trap when the transmission delay exceeds the threshold.

 **NOTE**

Parameters **owd-ds** and **owd-sd** can be configured only for jitter test instances.

**Step 4** Run:

```
commit
```

The configuration is committed.

----End

## 10.6 Checking the Configuration

### Context

After configuring the trap function, check the alarm information.

### Procedure

- Run the **display snmp-agent trap feature-name nqa all** command to check status of all traps on the NQA module.

----End

# 11 Scheduling an NQA Test Instance

---

## About This Chapter

After completing the configuration of an NQA test instance, you can schedule the NQA test instance, for example, starting the NQA test instance.

### Pre-configuration Tasks

Before scheduling an NQA test instance, complete the following tasks:

- Configure the server.
- Configure an NQA test instance on the client.
- Configure reachable routes between the server and the client.

 **NOTE**

Perform the following configurations on the NQA client:

[11.1 Starting an NQA Test Instance](#)

[11.2 \(Optional\) Stopping an NQA Test Instance](#)

[11.3 Checking Test Results](#)

## 11.1 Starting an NQA Test Instance

### Context

After completing the configuration of an NQA test instance, start the NQA test instance in following modes:

- Start the NQA test instance immediately.
- Start the NQA test instance at a specified time.
- Start the NQA test instance after a delay.

If the test fails, restart the NQA test instance in the next time period.

#### NOTE

- If the number of running test instances reaches the maximum value defined by the system, the **start** command is invalid.
- For the same test instance, the **start now** command can be used again only when the previous test is complete.
- The specified time to start a test instance must be later than the current time of the device.

### Procedure

- Start an NQA test instance.

a. Run:

```
system-view
```

The system view is displayed.

b. Run:

```
nqa test-instance admin-name test-name
```

The NQA view is displayed.

c. Run:

```
start
```

The NQA test instance is started.

■ Run:

```
start now [ end { at [ yyyy/mm/dd ] hh:mm:ss | delay { seconds  
second | hh:mm:ss } | lifetime { seconds second | hh:mm:ss } } ]
```

The NQA test instance is started immediately.

■ Run:

```
start at [ yyyy/mm/dd ] hh:mm:ss [ end { at [ yyyy/mm/dd ] hh:mm:ss  
| delay { seconds second | hh:mm:ss } | lifetime { seconds second |  
hh:mm:ss } } ]
```

The NQA test instance is started in a specified time.

■ Run:

```
start delay { seconds second | hh:mm:ss } [ end { at [ yyyy/mm/dd ]  
hh:mm:ss | delay { seconds second | hh:mm:ss } | lifetime { seconds  
second | hh:mm:ss } } ]
```

The NQA test instance is started after a specified delay.



■ Run:

```
start daily hh:mm:ss to hh:mm:ss [ begin { yyyy-mm-dd | yyyy/mm/  
dd } ] [ end { yyyy-mm-dd | yyyy/mm/dd } ]
```

The NQA test instance is started at a fixed time every day.

d. Run:

```
commit
```

The configuration is committed.

● Restart an NQA test instance.

a. Run:

```
system-view
```

The system view is displayed.

b. Run:

```
nqa test-instance admin-name test-name
```

The NQA view is displayed.

c. Run:

```
restart
```

Then NQA test instance is restarted.

■ The **restart** command stops the running test instance and restart it.

■ The **restart** command functions the same as the **start now** command.

d. Run:

```
commit
```

The configuration is committed.

----End

## 11.2 (Optional) Stopping an NQA Test Instance

### Context

A running NQA test instance can stop in the following modes:

- The test stops automatically after all test packets are sent.
- Stop the NQA test instance at a specified time.
- Stop the NQA test instance after a delay.
- Start a test instance and stop it at specified time every day.

Stop a running NQA test instance using either of the following commands:

- Run the **undo start** command to stop the running NQA test instance.
- Run the **stop** command to stop the running NQA test instance.

### Procedure

- Run the **undo start** command.

a. Run:

```
system-view
```

- The system view is displayed.
- b. Run:  
`nqa test-instance admin-name test-name`
- The NQA view is displayed.
- c. Run:  
`undo start`
- The running NQA test instance is stopped.
- d. Run:  
`commit`
- The configuration is committed.
- Run the **stop** command.

a. Run:  
`system-view`

The system view is displayed.

b. Run:  
`nqa test-instance admin-name test-name`

The NQA view is displayed.

c. Run:  
`stop`

The running NQA test instance is stopped.

d. Run:  
`commit`

The configuration is committed.
- End

## 11.3 Checking Test Results

### Prerequisites

An NQA test instance has been configured and the NQA test has been completed.

#### NOTE

- The **display nqa results** command displays the test results of only the test instances that have been completed.
- The **display nqa results collection** command displays accumulative results of all test instances. Only the jitter tests support the query of accumulative results.
- The **display nqa results collection this** command displays accumulative results of all test instances. Only the jitter tests support the query of accumulative results.
- Failed Jitter tests are not recorded in the historical records.

### Procedure

- Run the **display nqa results [ collection ] [ test-instance admin-name test-name ]** command to check NQA test results.

- Run the **display nqa history** [ **test-instance** *admin-name test-name* ] command to check the historical records of NQA test instances.
- Run the **display nqa results** [ **collection** ] **this** command to check results of an NQA test in the specified test instance view.
- Run the **display nqa history this** command to check historical records of NQA tests in the specified test instance view.

----End

# 12 Maintaining NQA

---

## About This Chapter

### [12.1 Clearing NQA Test Statistics](#)

## 12.1 Clearing NQA Test Statistics

### Context

To obtain the latest test results, clear the current test results by running the following commands.



### NOTICE

- Statistics cannot be restored after being cleared. Confirm the action before you run the commands.
  - Statistics on the running test instance cannot be cleared.
- 

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
nqa test-instance admin-name test-name
```

The NQA view is displayed.

**Step 3** Run:

```
clear-records
```

The statistics about NQA test instances are cleared.

**Step 4** Run:

```
return
```

Return to the user view.

----End

# 13 Configuration Examples

---

## About This Chapter

- [13.1 Example for Configuring an ICMP Test Instance](#)
- [13.2 Example for Configuring an ICMP Jitter Test Instance](#)
- [13.3 Example for Configuring a TCP Test Instance](#)
- [13.4 Example for Configuring Trace Test](#)
- [13.5 Example for Configuring a UDP Jitter Test Instance](#)
- [13.6 Example for Configuring LSP Ping Test for LSP Tunnels](#)
- [13.7 Example for Configuring LSP Trace Test for LSP Tunnels](#)

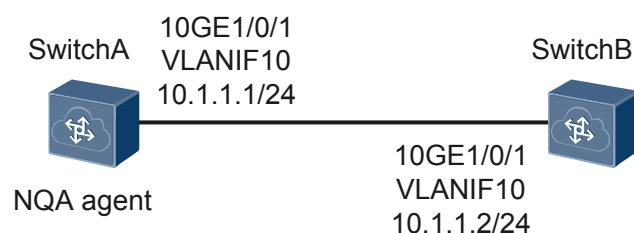
## 13.1 Example for Configuring an ICMP Test Instance

### Networking Requirements

In [Figure 13-1](#), SwitchA, SwitchB, and SwitchC communicate at Layer 3 using VLANIF interfaces.

SwitchA functions as an NQA client to test whether SwitchB is reachable.

**Figure 13-1** Networking diagram for configuring an ICMP test instance



### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an NQA ICMP test instance to test whether the route between the local device (SwitchA) and the specified destination device (SwitchB) is reachable and check the RTT of a test packet.

### Procedure

**Step 1** Create VLANs and add interfaces to the VLANs.

# Configure SwitchA.

```

<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] vlan 10
[*SwitchA-vlan10] quit
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] port link-type trunk
[*SwitchA-10GE1/0/1] port trunk pvid vlan 10
[*SwitchA-10GE1/0/1] port trunk allow-pass vlan 10
[*SwitchA-10GE1/0/1] commit
[~SwitchA-10GE1/0/1] quit
  
```

# Configure SwitchB.

```

<HUAWEI> system-view
[~HUAWEI] sysname SwitchB
[*HUAWEI] commit
[~SwitchB] vlan 10
[*SwitchB-vlan10] quit
[*SwitchB] interface 10ge 1/0/1
[*SwitchB-10GE1/0/1] port link-type trunk
[*SwitchB-10GE1/0/1] port trunk pvid vlan 10
  
```

```
[*SwitchB-10GE1/0/1] port trunk allow-pass vlan 10
[*SwitchB-10GE1/0/1] commit
[~SwitchB-10GE1/0/1] quit
```

**Step 2** Create VLANIF interfaces and assign IP addresses to the VLANIF interfaces.

# Configure SwitchA.

```
[~SwitchA] interface vlanif 10
[*SwitchA-Vlanif10] ip address 10.1.1.1 24
[*SwitchA-Vlanif10] commit
[~SwitchA-Vlanif10] quit
```

# Configure SwitchB.

```
[~SwitchB] interface vlanif 10
[*SwitchB-Vlanif10] ip address 10.1.1.2 24
[*SwitchB-Vlanif10] commit
[~SwitchB-Vlanif10] quit
```

**Step 3** Enable the NQA client and create an ICMP NQA test instance.

```
[~SwitchA] nqa test-instance admin icmp
[*SwitchA-nqa-admin-icmp] test-type icmp
[*SwitchA-nqa-admin-icmp] destination-address ipv4 10.1.1.2
[*SwitchA-nqa-admin-icmp] commit
```

**Step 4** Start the test instance immediately.

```
[~SwitchA-nqa-admin-icmp] start now
[*SwitchA-nqa-admin-icmp] commit
```

**Step 5** Verify the configuration.

```
[~SwitchA-nqa-admin-icmp] display nqa results test-instance admin icmp

NQA entry(admin, icmp): test flag is active, test type is ICMP
 1 . Test 1 result The test is finished
  Send operation times: 3          Receive response times: 3
  Completion: success           RTD over thresholds number: 0
  Attempts number: 1           Drop operation number: 0
  Disconnect operation number: 0 Operation timeout number: 0
  System busy operation number: 0 Connection fail number: 0
  Operation sequence errors number: 0 RTT Status errors number: 0
  Destination IP address: 10.1.1.2
  Min/Max/Average completion time: 2/5/3
  Sum/Square-Sum completion time: 9/33
  Last response packet receiving time: 2012-08-08
15:53:08.4
  Lost packet ratio: 0 %
```

----End

## Configuration Files

- SwitchA configuration file

```
#
sysname SwitchA
#
vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 10
 port trunk allow-pass vlan 10
#
nqa test-instance admin icmp
```



```
test-type icmp
destination-address ipv4 10.1.1.2
#
return
```

- SwitchB configuration file

```
#
sysname SwitchB
#
vlan batch 10
#
interface Vlanif10
ip address 10.1.1.2 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk pvid vlan 10
port trunk allow-pass vlan 10
#
return
```

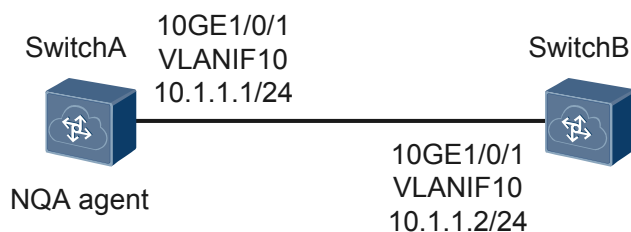
## 13.2 Example for Configuring an ICMP Jitter Test Instance

### Networking Requirements

In [Figure 13-2](#), SwitchA, SwitchB, and SwitchC communicate at Layer 3 using VLANIF interfaces.

SwitchA functions as the NQA client to test the jitter of the network between SwitchA and SwitchB.

**Figure 13-2** Networking diagram for configuring an ICMP jitter test instance



### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure SwitchA as an NQA client and create an ICMP jitter test instance on SwitchA.

### Procedure

- Step 1** Create VLANs and add interfaces to the VLANs.

# Configure SwitchA.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
```

```
[~SwitchA] vlan 10
[*SwitchA-vlan10] quit
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] port link-type trunk
[*SwitchA-10GE1/0/1] port trunk pvid vlan 10
[*SwitchA-10GE1/0/1] port trunk allow-pass vlan 10
[*SwitchA-10GE1/0/1] commit
[~SwitchA-10GE1/0/1] quit
```

#### # Configure SwitchB.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchB
[*HUAWEI] commit
[~SwitchB] vlan 10
[*SwitchB-vlan10] quit
[*SwitchB] interface 10ge 1/0/1
[*SwitchB-10GE1/0/1] port link-type trunk
[*SwitchB-10GE1/0/1] port trunk pvid vlan 10
[*SwitchB-10GE1/0/1] port trunk allow-pass vlan 10
[*SwitchB-10GE1/0/1] commit
[~SwitchB-10GE1/0/1] quit
```

### Step 2 Create VLANIF interfaces and assign IP addresses to the VLANIF interfaces.

#### # Configure SwitchA.

```
[~SwitchA] interface vlanif 10
[*SwitchA-Vlanif10] ip address 10.1.1.1 24
[*SwitchA-Vlanif10] commit
[~SwitchA-Vlanif10] quit
```

#### # Configure SwitchB.

```
[~SwitchB] interface vlanif 10
[*SwitchB-Vlanif10] ip address 10.1.1.2 24
[*SwitchB-Vlanif10] commit
[~SwitchB-Vlanif10] quit
```

### Step 3 # Enable the NQA client and create an ICMP jitter NQA test instance.

```
[~SwitchA] nqa test-instance admin icmpjitter
[*SwitchA-nqa-admin-icmpjitter] test-type icmpjitter
[*SwitchA-nqa-admin-icmpjitter] destination-address ipv4 10.1.1.2
[*SwitchA-nqa-admin-icmpjitter] commit
```

### Step 4 Start the test instance immediately.

```
[~SwitchA-nqa-admin-icmpjitter] start now
[*SwitchA-nqa-admin-icmpjitter] commit
```

### Step 5 Verify the configuration.

```
[~SwitchA-nqa-admin-icmpjitter] display nqa results test-instance admin icmpjitter

NQA entry(admin, icmpjitter): test flag is inactive, test type is ICMPJITTER
 1 . Test 1 result The test is finished
  SendProbe: 60 ResponseProbe: 60
  Completion: success RTD over thresholds number: 0
  OWD over thresholds SD number: 0 OWD over thresholds DS number: 0
  Min/Max/Avg/Sum RTT: 1/5/2/128 RTT square sum: 294
  Num of RTT: 60 Drop operation number: 0
  Operation sequence errors number: 0 RTT Status errors number: 0
  System busy operation number: 0 Operation timeout number: 0
  Min positive SD: 1 Min positive DS: 1
  Max positive SD: 3 Max positive DS: 1
  Positive SD number: 10 Positive DS number: 9
  Positive SD sum: 12 Positive DS sum: 9
  Positive SD square sum: 18 Positive DS square sum: 9
  Min negative SD: 1 Min negative DS: 1
```

```

Max negative SD: 4
Negative SD number: 10
Negative SD sum: 13
Negative SD square sum: 25
Min delay SD: 1
Avg delay SD: 0
Max delay SD: 2
Delay SD square sum: 59
Packet loss SD: 0
Packet loss unknown: 0
Average of jitter SD: 1
Jitter out value: 0.3360330
Number of OWD: 60
OWD SD sum: 57
ICPIF value: 0
TimeStamp unit: ms

Max negative DS: 5
Negative DS number: 9
Negative DS sum: 13
Negative DS square sum: 33
Min delay DS: 0
Avg delay DS: 0
Max delay DS: 2
Delay DS square sum: 13
Packet loss DS: 0
Average of jitter: 1
Average of jitter DS: 1
Jitter in value: 0.3163250
Packet loss ratio: 0 %
OWD DS sum: 11
MOS-CQ value: 0
  
```

----End

## Configuration Files

- SwitchA configuration file

```

#
sysname SwitchA
#
vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 10
 port trunk allow-pass vlan 10
#
nqa test-instance admin icmpjitter
 test-type icmpjitter
 destination-address ipv4 10.1.1.2
#
return
  
```

- SwitchB configuration file

```

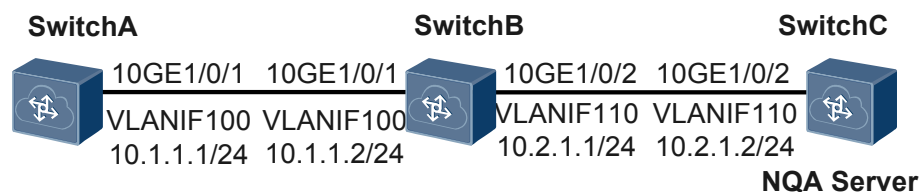
#
sysname SwitchB
#
vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 10
 port trunk allow-pass vlan 10
#
return
  
```

## 13.3 Example for Configuring a TCP Test Instance

### Networking Requirements

The NQA TCP test instance is used to obtain the time for setting up a TCP connection between SwitchA and SwitchC, as shown in the [Figure 13-3](#).

**Figure 13-3** Networking diagram for configuring a TCP test instance



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure switchA as an NQA client and SwitchC as an NQA server.
2. Configure the monitoring port number on the NQA server and create an NQA TCP test instance on the NQA client.

## Procedure

- Step 1** Configure each interface and ensure reachable routes between Switches, as shown in [Figure 13-3](#).

# Configure SwitchA. The configurations of SwitchB and SwitchC are similar to the configuration of SwitchA.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] vlan 100
[*SwitchA-vlan100] quit
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] port link-type trunk
[*SwitchA-10GE1/0/1] port trunk pvid vlan 100
[*SwitchA-10GE1/0/1] port trunk allow-pass vlan 100
[*SwitchA-10GE1/0/1] quit
[*SwitchA] interface vlanif 100
[*SwitchA-Vlanif100] ip address 10.1.1.1 24
[*SwitchA-Vlanif100] quit
[*SwitchA] quit
[*SwitchA] ip route-static 10.2.1.0 24 10.1.1.2
[*SwitchA] commit
```

- Step 2** Configure the NQA server on SwitchC.

# Configure the IP address and port number for monitoring TCP connections on the NQA server.

```
<SwitchC> system-view
[~SwitchC] nqa server tcpconnect 10.2.1.2 9000
[*SwitchC] commit
```

- Step 3** Configure SwitchA.

# Enable the NQA client and create a TCP Private test instance.

```
[~SwitchA] nqa test-instance admin tcp
[*SwitchA-nqa-admin-tcp] test-type tcp
[*SwitchA-nqa-admin-tcp] destination-address ipv4 10.2.1.2
[*SwitchA-nqa-admin-tcp] destination-port 9000
[*SwitchA-nqa-admin-tcp] commit
```

**Step 4 Start the test instance.**

```
[~SwitchA-nqa-admin-tcp] start now
[*SwitchA-nqa-admin-tcp] commit
```

**Step 5 Verify the configuration.**

```
[~SwitchA-nqa-admin-tcp] display nqa results test-instance admin tcp

NQA entry(admin, tcp): test flag is active, test type is TCP
 1 . Test 1 result The test is finished
  Send operation times: 3          Receive response times: 3
  Completion: success           RTD over thresholds number: 0
  Attempts number: 1            Drop operation number: 0
  Disconnect operation number: 0 Operation timeout number: 0
  System busy operation number: 0 Connection fail number: 0
  Operation sequence errors number: 0 RTT Status errors number: 0
  Destination IP address: 10.2.1.2
  Min/Max/Average completion time: 103/133/114
  Sum/Square-Sum completion time: 343/39747
  Last response packet receiving time: 2012-08-09
00:24:06.1
  Lost packet ratio: 0 %
```

---End

## Configuration Files

- SwitchA configuration file

```
#
sysname SwitchA
#
vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
nqa test-instance admin tcp
 test-type tcp
 destination-address ipv4 10.2.1.2
 destination-port 9000
#
return
```

- SwitchB configuration file

```
#
sysname SwitchB
#
vlan batch 100 110
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif110
 ip address 10.2.1.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
#
interface 10GE1/0/2
```

```
port link-type trunk
port trunk pvid vlan 110
port trunk allow-pass vlan 110
#
return
```

- SwitchC configuration file

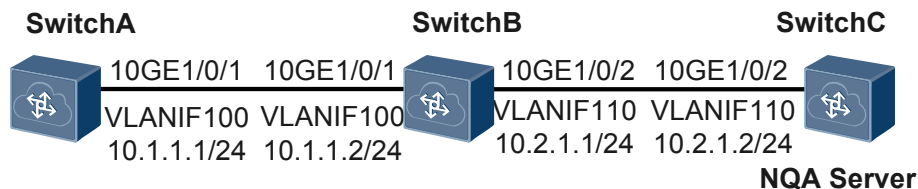
```
#
sysname SwitchC
#
vlan batch 110
#
interface Vlanif110
ip address 10.2.1.2 255.255.255.0
#
interface 10GE1/0/2
port link-type trunk
port trunk pvid vlan 110
port trunk allow-pass vlan 110
#
nqa server tcpconnect 10.2.1.2 9000
#
ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

## 13.4 Example for Configuring Trace Test

### Networking Requirements

In **Figure 13-4**, the trace test is configured on SwitchA to test the IP address of the VLANIF 110 interface of SwitchC.

**Figure 13-4** Networking diagram for configuring the trace test



### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure SwitchA as the NQA client. Create and perform the trace test on SwitchA to check the statistics on each hop from SwitchA to SwitchC.

### Procedure

- Step 1** Configure an IP address for each interface according to **Figure 13-4**, and configure reachable routes from one Switch to another.

# Configure SwitchA. The configurations of SwitchB and SwitchC are similar to the configuration of SwitchA.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
```

```
[*HUAWEI] commit
[~SwitchA] vlan 100
[*SwitchA-vlan100] quit
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] port link-type trunk
[*SwitchA-10GE1/0/1] port trunk pvid vlan 100
[*SwitchA-10GE1/0/1] port trunk allow-pass vlan 100
[*SwitchA-10GE1/0/1] quit
[*SwitchA] interface vlanif 100
[*SwitchA-Vlanif100] ip address 10.1.1.1 24
[*SwitchA-Vlanif100] quit
[*SwitchA] ip route-static 10.2.1.0 24 10.1.1.2
[*SwitchA] commit
```

**Step 2** Create an NQA trace test instance on SwitchA and set the destination IP address to 10.2.1.2.

```
[~SwitchA] nqa test-instance admin trace
[*SwitchA-nqa-admin-trace] test-type trace
[*SwitchA-nqa-admin-trace] destination-address ipv4 10.2.1.2
[*SwitchA-nqa-admin-trace] commit
```

**Step 3** Start NQA test instances.

```
[~SwitchA-nqa-admin-trace] start now
[*SwitchA-nqa-admin-trace] commit
```

**Step 4** Query test results.

# View the NQA test result on SwitchA. (V100R005C00)

```
[~SwitchA-nqa-admin-trace] display nqa results test-instance admin trace

NQA entry(admin, trace): test flag is inactive, test type is TRACE
 1 . Test 1 result The test is finished
    Completion:success                Attempts number:1
    Disconnect operation number:0      Operation timeout number:0
    System busy operation number:0     Connection fail number:0
    Operation sequence errors number:0 RTT Status errors number:0
    Drop operation number:0
    Last good path Time: 2015-03-16 16:29:26.8
 1 . Hop 1
    Send operation times: 3            Receive response times: 3
    Min/Max/Average Completion Time: 3/20/9
    Sum/Square-Sum Completion Time: 28/434
    RTD OverThresholds number:0
    Last Good Probe Time: 2015-03-16 16:29:26.7
    Destination ip address:10.1.1.2
    Lost packet ratio: 0 %
 2 . Hop 2
    Send operation times: 3            Receive response times: 3
    Min/Max/Average Completion Time: 2/10/5
    Sum/Square-Sum Completion Time: 15/113
    RTD OverThresholds number:0
    Last Good Probe Time: 2015-03-16 16:29:26.8
    Destination ip address:10.2.1.2
    Lost packet ratio: 0 %
```

----End

## Configuration File

- SwitchA configuration file

```
#
sysname SwitchA
#
vlan batch 100
#
interface Vlanif100
ip address 10.1.1.1 255.255.255.0
```

```
#
interface 10GE1/0/1
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100
#
ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
nqa test-instance admin trace
test-type trace
destination-address ipv4 10.2.1.2
#
return
```

- SwitchB configuration file

```
#
sysname SwitchB
#
vlan batch 100 110
#
interface Vlanif100
ip address 10.1.1.2 255.255.255.0
#
interface Vlanif110
ip address 10.2.1.1 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100
#
interface 10GE1/0/2
port link-type trunk
port trunk pvid vlan 110
port trunk allow-pass vlan 110
#
return
```

- SwitchC configuration file

```
#
sysname SwitchC
#
vlan batch 110
#
interface Vlanif110
ip address 10.2.1.2 255.255.255.0
#
interface 10GE1/0/2
port link-type trunk
port trunk pvid vlan 110
port trunk allow-pass vlan 110
#
ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

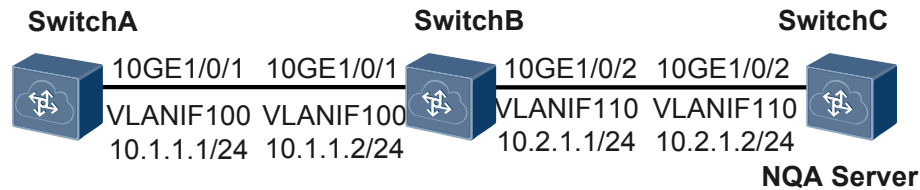
## 13.5 Example for Configuring a UDP Jitter Test Instance

### Networking Requirements

The NQA jitter test instance is used to obtain the jitter time of transmitting a packet from SwitchA to SwitchC, as shown in [Figure 13-5](#).



**Figure 13-5** Networking diagram for configuring a UDP Jitter test instance



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure SwitchA as an NQA client and SwitchC as an NQA server.
2. Configure the monitoring IP address and port number on the NQA server, and configure a jitter test instance on the NQA client.

## Procedure

- Step 1** Configure each interface and ensure reachable routes between Switches, as shown in [Figure 13-5](#).

# Configure SwitchA. The configurations of SwitchB and SwitchC are similar to the configuration of SwitchA.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] vlan 100
[*SwitchA-vlan100] quit
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] port link-type trunk
[*SwitchA-10GE1/0/1] port trunk pvid vlan 100
[*SwitchA-10GE1/0/1] port trunk allow-pass vlan 100
[*SwitchA-10GE1/0/1] quit
[*SwitchA] interface vlanif 100
[*SwitchA-Vlanif100] ip address 10.1.1.1 24
[*SwitchA-Vlanif100] quit
[*SwitchA] quit
[*SwitchA] ip route-static 10.2.1.0 24 10.1.1.2
[*SwitchA] commit
```

- Step 2** Configure the NQA server on SwitchC.

# Configure the IP address and port number for monitoring UDP services on the NQA server.

```
<SwitchC> system-view
[~SwitchC] nqa server udpecho 10.2.1.2 9000
[*SwitchC] commit
```

- Step 3** Configure SwitchA.

# Enable the NQA client and create an NQA jitter test instance.

```
[~SwitchA] nqa test-instance admin jitter
[*SwitchA-nqa-admin-jitter] test-type jitter
[*SwitchA-nqa-admin-jitter] destination-address ipv4 10.2.1.2
[*SwitchA-nqa-admin-jitter] destination-port 9000
[*SwitchA-nqa-admin-jitter] commit
```

**Step 4 Start the test instance.**

```
[~SwitchA-nqa-admin-jitter] start now
[*SwitchA-nqa-admin-jitter] commit
```

**Step 5 Verify the configuration.**

```
[~SwitchA-nqa-admin-jitter] display nqa results test-instance admin jitter

NQA entry(admin, jitter): test flag is inactive, test type is JITTER
 1 . Test 1 result The test is finished
  SendProbe: 60 ResponseProbe: 60
  Completion: success RTD over thresholds number: 0
  OWD over thresholds SD number: 0 OWD over thresholds DS number: 0
  Min/Max/Avg/Sum RTT: 2/77/7/401 RTT square sum: 11877
  Num of RTT: 60 Drop operation number: 0
  Operation sequence errors number: 0 RTT Status errors number: 0
  System busy operation number: 0 Operation timeout number: 0
  Min positive SD: 1 Min positive DS: 1
  Max positive SD: 10 Max positive DS: 2
  Positive SD number: 7 Positive DS number: 14
  Positive SD sum: 16 Positive DS sum: 16
  Positive SD square sum: 106 Positive DS square sum: 20
  Min negative SD: 1 Min negative DS: 1
  Max negative SD: 10 Max negative DS: 21
  Negative SD number: 9 Negative DS number: 18
  Negative SD sum: 18 Negative DS sum: 88
  Negative SD square sum: 108 Negative DS square sum: 1368
  Min delay SD: 1 Min delay DS: 0
  Avg delay SD: 3 Avg delay DS: 2
  Max delay SD: 38 Max delay DS: 38
  Delay SD square sum: 2858 Delay DS square sum: 2723
  Packet loss SD: 0 Packet loss DS: 0
  Packet loss unknown: 0 Average of jitter: 2
  Average of jitter SD: 2 Average of jitter DS: 3
  Jitter out value: 0.4763590 Jitter in value: 1.5859300
  Number of OWD: 60 Packet loss ratio: 0 %
  OWD SD sum: 184 OWD DS sum: 157
  ICPIF value: 0 MOS-CQ value: 0
  TimeStamp unit: ms
```

----End

## Configuration Files

- SwitchA configuration file

```
#
sysname SwitchA
#
vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 10.2.1.2
 destination-port 9000
#
return
```

- SwitchB configuration file

```
#
sysname SwitchB
#
vlan batch 100 110
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif110
 ip address 10.2.1.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
#
interface 10GE1/0/2
 port link-type trunk
 port trunk pvid vlan 110
 port trunk allow-pass vlan 110
#
return
```

- SwitchC configuration file

```
#
sysname SwitchC
#
vlan batch 110
#
interface Vlanif110
 ip address 10.2.1.2 255.255.255.0
#
interface 10GE1/0/2
 port link-type trunk
 port trunk pvid vlan 110
 port trunk allow-pass vlan 110
#
nqa server udpecho 10.2.1.2 9000
#
ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

## 13.6 Example for Configuring LSP Ping Test for LSP Tunnels

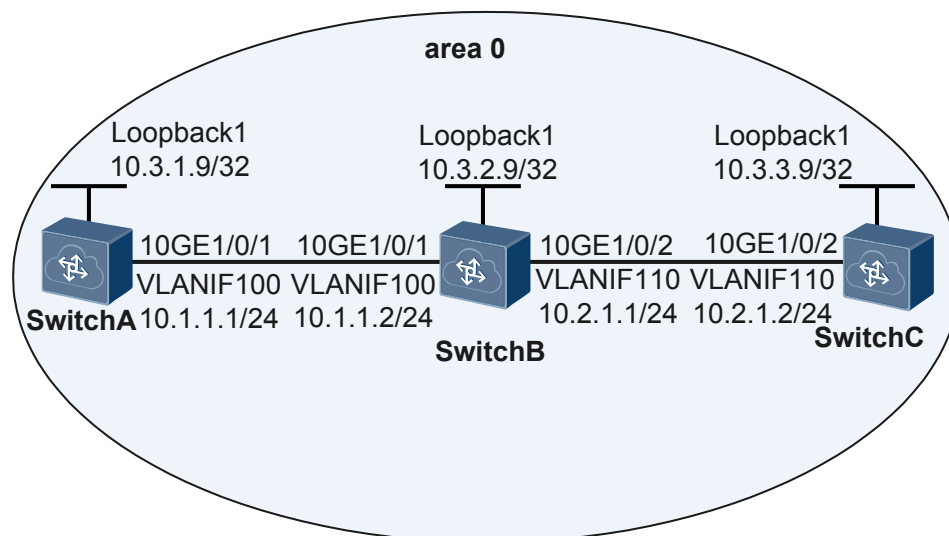
### Networking Requirements

In [Figure 13-6](#),

- SwitchA, SwitchB, and SwitchC run the OSPF protocol, and has learned the 32-bit host routes of the loopback interface of each other.
- MPLS and MPLS LDP are enabled on SwitchA, SwitchB, and SwitchC.
- MPLS and MPLS LDP are enabled on the VLANIF interfaces between SwitchA, SwitchB, and SwitchC to trigger the establishment of an LDP LSP.

The NQA LSP Ping test needs to be performed to check the connectivity of the LSP between SwitchA and SwitchC.

Figure 13-6 Networking diagram of an LSP Ping test



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure SwitchA as the NQA client.
2. Configure SwitchC as the NQA server.
3. Configure an LSP Ping test instance on SwitchA.

## Procedure

**Step 1** Configure the routes and LDP sessions between SwitchA, SwitchB, and SwitchC.

For the detailed configurations, see the configuration files of SwitchA, SwitchB, and SwitchC.

**Step 2** Configure an LSP Ping test instance.

# Enable the NQA client and create an LSP Ping test instance for LSP tunnels.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] nqa test-instance admin lsping
[*SwitchA-nqa-admin-lsping] test-type lsping
[*SwitchA-nqa-admin-lsping] lsp-type ipv4
[*SwitchA-nqa-admin-lsping] destination-address ipv4 10.3.3.9 lsp-masklen 32
[*SwitchA-nqa-admin-lsping] commit
```

**Step 3** Start the test instance.

```
[~SwitchA-nqa-admin-lsping] start now
[*SwitchA-nqa-admin-lsping] commit
```

**Step 4** Verify the test result.

```
[~SwitchA-nqa-admin-lsping] display nqa results test-instance admin lsping

NQA entry(admin, lsping): test flag is inactive, test type is LSPPING
 1 . Test 1 result The test is finished
```

```

Send operation times: 3          Receive response times: 3
Completion: success            RTD over thresholds number: 0
Attempts number: 1             Drop operation number: 0
Disconnect operation number: 0 Operation timeout number: 0
System busy operation number: 0 Connection fail number: 0
Operation sequence errors number: 0 RTT Status errors number: 0
Destination IP address: 10.3.3.9
Min/Max/Average completion time: 4/5/4
Sum/Square-Sum completion time: 13/57
Last response packet receiving time: 2013-12-09 08:57:55.6
Lost packet ratio: 0 %
  
```

----End

## Configuration File

- SwitchA configuration file

```

#
sysname SwitchA
#
vlan batch 100
#
mpls lsr-id 10.3.1.9
#
mpls
#
mpls ldp
#
ipv4-family
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
#
interface LoopBack1
 ip address 10.3.1.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.3.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
nqa test-instance admin lspping
 test-type lspping
 destination-address ipv4 10.3.3.9 lsp-masklen 32
#
return
  
```

- SwitchB configuration file

```

#
sysname SwitchB
#
vlan batch 100 110
#
mpls lsr-id 10.3.2.9
#
mpls
#
mpls ldp
#
ipv4-family
#
  
```

```

interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlanif110
 ip address 10.2.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
#
interface 10GE1/0/2
 port link-type trunk
 port trunk pvid vlan 110
 port trunk allow-pass vlan 110
#
interface LoopBack1
 ip address 10.3.2.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.3.2.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
#
return
  
```

- SwitchC configuration file

```

#
sysname SwitchC
#
vlan batch 110
#
mpls lsr-id 10.3.3.9
#
mpls
#
mpls ldp
#
 ipv4-family
#
interface Vlanif110
 ip address 10.2.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface 10GE1/0/2
 port link-type trunk
 port trunk pvid vlan 110
 port trunk allow-pass vlan 110
#
interface LoopBack1
 ip address 10.3.3.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.3.3.9 0.0.0.0
  network 10.2.1.0 0.0.0.255
#
return
  
```

## 13.7 Example for Configuring LSP Trace Test for LSP Tunnels

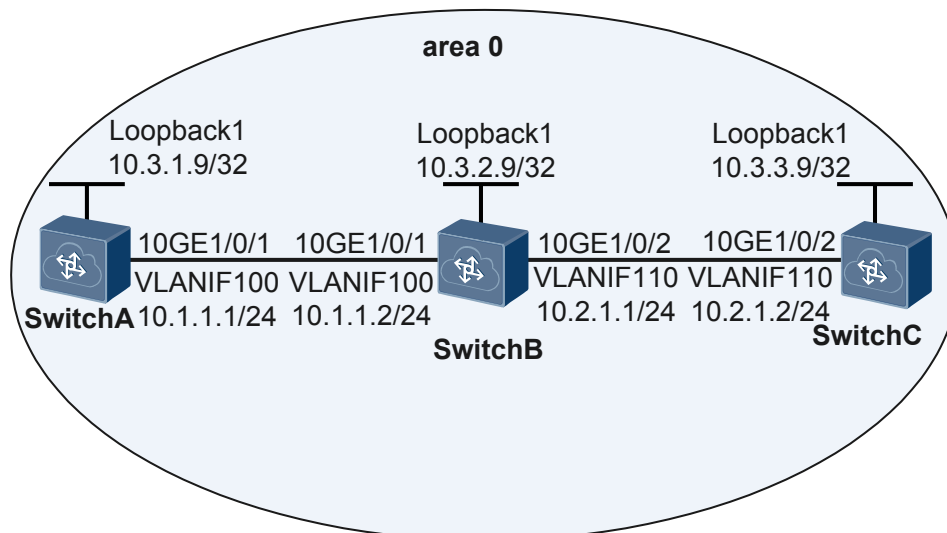
### Networking Requirements

In [Figure 13-7](#),

- SwitchA, SwitchB, and SwitchC run the OSPF protocol and has learned the 32-bit host routes of the loopback interfaces of each other.
- MPLS and MPLS LDP are enabled on SwitchA, SwitchB, and SwitchC.
- MPLS and MPLS LDP are enabled on the VLANIF interfaces between SwitchA, SwitchB, and SwitchC to trigger the establishment of an LDP LSP.

The NQA LSP Trace test needs to be performed to test the LSP paths.

**Figure 13-7** Networking diagram for configuring the LSP Trace test



### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure SwitchA as the NQA client.
2. Configure SwitchC as the NQA server.
3. Configure an LSP Trace test instance on SwitchA.

### Procedure

**Step 1** Configure the routes and LDP sessions between SwitchA, SwitchB, and SwitchC.

For the detailed configurations, see the configuration files of SwitchA, SwitchB, and SwitchC.

## Step 2 Configure an LSP Trace test instance.

# Enable the NQA client and create an LSP Trace test instance for LSP tunnels.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] nqa test-instance admin lsptrace
[*SwitchA-nqa-admin-lsptrace] test-type lsptrace
[*SwitchA-nqa-admin-lsptrace] lsp-type ipv4
[*SwitchA-nqa-admin-lsptrace] destination-address ipv4 10.3.3.9 lsp-masklen 32
[*SwitchA-nqa-admin-lsptrace] commit
```

## Step 3 Start the test instance.

```
[~SwitchA-nqa-admin-lsptrace] start now
[*SwitchA-nqa-admin-lsptrace] commit
```

## Step 4 Verify the test result.

```
[~SwitchA-nqa-admin-lsptrace] display nqa results test-instance admin lsptrace

NQA entry(admin, lsptrace): test flag is inactive, test type is LSPTRACE
 1 . Test 1 result The test is finished
    Completion:success                               Attempts number:1
    Disconnect operation number:0                     Operation timeout number:0
    System busy operation number:0                   Connection fail number:0
    Operation sequence errors number:0               RTT stats errors number:0
    Drop operation number:0
    Last good path Time: 2013-12-09 08:58:14.9
 1 . Hop 1
    Send operation times: 3                           Receive response times: 3
    Min/Max/Average completion time: 2/7/4
    Sum/Square-Sum completion time: 12/62
    RTD over thresholds number:0
    Last response packet receive time: 2013-12-09 08:58:14.9
    Destination IP address:10.1.1.2
    Lost packet ratio: 0 %
 2 . Hop 2
    Send operation times: 3                           Receive response times: 3
    Min/Max/Average completion time: 2/3/2
    Sum/Square-Sum completion time: 7/17
    RTD over thresholds number:0
    Last response packet receive time: 2013-12-09 08:58:14.9
    Destination IP address:10.3.3.9
    Lost packet ratio: 0 %
```

---End

## Configuration File

- SwitchA configuration file

```
#
sysname SwitchA
#
vlan batch 100
#
mpls lsr-id 10.3.1.9
#
mpls
#
mpls ldp
#
ipv4-family
#
interface Vlanif100
ip address 10.1.1.1 255.255.255.0
mpls
mpls ldp
```



```
#
interface 10GE1/0/1
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100
#
interface LoopBack1
ip address 10.3.1.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 10.3.1.9 0.0.0.0
network 10.1.1.0 0.0.0.255
#
nqa test-instance admin lsptrace
test-type lsptrace
destination-address ipv4 10.3.3.9 lsp-masklen 32
#
return
```

- SwitchB configuration file

```
#
sysname SwitchB
#
vlan batch 100 110
#
mpls lsr-id 10.3.2.9
#
mpls
#
mpls ldp
#
ipv4-family
#
interface Vlanif100
ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Vlanif110
ip address 10.2.1.1 255.255.255.0
mpls
mpls ldp
#
interface 10GE1/0/1
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100
#
interface 10GE1/0/2
port link-type trunk
port trunk pvid vlan 110
port trunk allow-pass vlan 110
#
interface LoopBack1
ip address 10.3.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 10.3.2.9 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.2.1.0 0.0.0.255
#
return
```

- SwitchC configuration file

```
#
sysname SwitchC
#
vlan batch 110
```

```
#
mpls lsr-id 10.3.3.9
#
mpls
#
mpls ldp
#
  ipv4-family
#
interface Vlanif110
  ip address 10.2.1.2 255.255.255.0
  mpls
  mpls ldp
#
interface 10GE1/0/2
  port link-type trunk
  port trunk pvid vlan 110
  port trunk allow-pass vlan 110
#
interface LoopBack1
  ip address 10.3.3.9 255.255.255.255
#
ospf 1
  area 0.0.0.0
    network 10.3.3.9 0.0.0.0
    network 10.2.1.0 0.0.0.255
#
return
```

# 14 References

The following lists the references for NAQ.

Document	Description	Remarks
RFC 1889	RTP: A Transport Protocol for Real-Time Applications	-
RFC 2925	Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations	-
RFC 2131	Dynamic Host Configuration Protocol	-
RFC 1035	DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION	-
RFC 414	FILE TRANSFER PROTOCOL (FTP) STATUS AND FURTHER COMMENTS	-
RFC 1945	Hypertext Transfer Protocol - HTTP/1.0	-
RFC 2616	Hypertext Transfer Protocol - HTTP/1.1	-
RFC 792	INTERNET CONTROL MESSAGE PROTOCOL	-
RFC 4379	Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures	-
IEEE 802.1AG DRAFT6.1	IEEE 802.1AG DRAFT6.1	-
DRAFT-FENNER-TRACEROUTE-IPM-07	DRAFT-FENNER-TRACEROUTE-IPM-07	-
RFC 1157	A Simple Network Management Protocol (SNMP)	-
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)	-

Document	Description	Remarks
RFC 1905	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)	-
RFC793	Transmission Control Protocol	TCP/UDP test
RFC 862	Echo Protocol	TCP/UDP test
RFC 1393	Traceroute Using an IP Option	Trace test