Contents

1 Configuring Network Connectivity Test

1.1 Introduction

1.1.1 Overview

The network connectivity test tool is used to check whether the network can be connected, and accurately find out the cause of the network failure. Common network communication test tools include packet Internet groper (Ping) and Traceroute. On a network device, the commands corresponding to these two tools are **ping** and **traceroute**.

● The Ping tool is often used to check the network connectivity between devices and the network delay. A larger delay indicates a slower network speed.

● The Traceroute tool helps users learn the topology of the physical and logical connections of the network and efficiency of data transmission.

1.1.2 Principles

1. Testing connectivity with Ping

The Ping tool sends an Internet Control Message Protocol (ICMP) Echo Request packet to the destination IP address, requesting the peer to return an ICMP Echo Reply packet to determine whether the two network devices are connected and what is the delay.

The sequence number of the ICMP Echo Request starts from 0. Each time an ICMP Echo Request is sent by the Ping tool, the sequence number increases by 1. The sender sends five ICMP Echo Request packets by default. You can also specify the number of sent ICMP Echo Request packets in the command. If two devices are connected, the receiver returns the same number of ICMP Echo Reply packets.

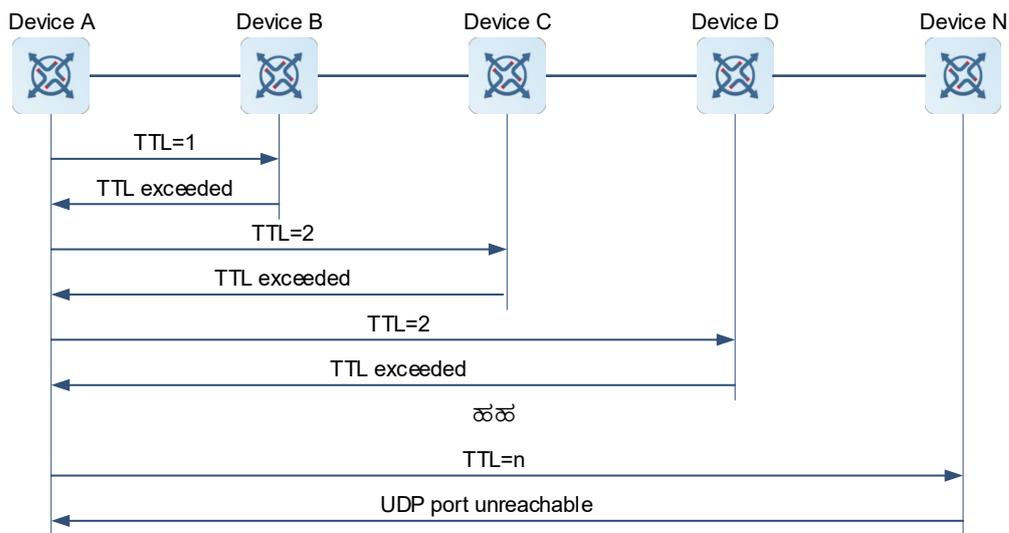**Figure 1-1   Testing Connectivity with Ping**
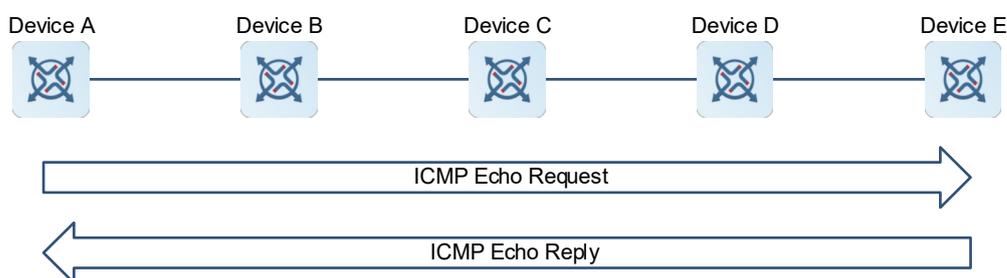
2. Testing connectivity with Traceroute

The Traceroute tool uses the Time To Live (TTL) field in the header of ICMP and IP packets to complete the connectivity check. The process is as follows:

Figure 1-1   Testing Connectivity with Traceroute

(1) Device A sends an ICMP Request packet with the TTL set to 1 through the Traceroute tool. The UDP port number in the packet is an invalid destination port number (greater than 3000).

(2) When the first device, device B, on the path receives this packet, device B decreases the TTL by 1. Then, the TTL changes to 0, and the device discards the packet and returns an ICMP Time Exceeded message.

(3) When Traceroute on device A receives this message, it learns that device B exists on the path and therefore sends a packet with the TTL set to 2 to detect the second device, device C.

(4) Each time when device A sends a packet, Traceroute on device A increases the TTL by 1 to detect another device. This operation repeats until a packet arrives at the destination host. When the packet arrives at the destination host, the host returns an ICMP Port Unreachable message, instead of an ICMP Time Exceeded message. Finally, Traceroute stops the detection and displays the path from the network device to the destination host.

1.1.3 Protocols and Standards

- RFC792: Internet Control Message Protocol
- RFC4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

1.2 Restrictions and Guidelines

An IP address must be configured for the network device where the Ping and Traceroute operations are executed.

1.3 Configuration Task Summary

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring a Ping Connectivity Test
- Configuring a Traceroute Connectivity Test

1.4 Configuring a Ping Connectivity Test

1.4.1 Overview

You can use Ping connectivity test to check whether a network device is connected to the destination host and whether packets can be transmitted between these two devices.

1.4.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Check whether the IP address is reachable.

(IPv4 network)

ping [**ip** | **vrf** *vrf-name*] { *hostname* | *ipv4-address* } [**data** *data* | **detail** | **df-bit** | **interval** *interval* | **length** *length* | **ntimes** *times* | **out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | [**source** *interface-type interface-number* | **source** *source-ipv4-address*] | **timeout** *time* | **validate**] *

(IPv6 network)

ping [**ipv6** | **vrf** *vrf-name*] { *hostname* | ipv6-*address* } [**data** *data* | **detail** | **interval** *interval* | **length** *length* | **ntimes** *times* | **out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | [**source** *interface-type interface-number* | **source** *source-ipv6-address*] | **timeout** *time*] *

By default, five 100-byte packets are sent to the specified IP address within two seconds.

1.5 Configuring a Traceroute Connectivity Test

1.5.1 Overview

You can use Traceroute connectivity test on a network device to learn the routing topology and the number of gateways between this device and the destination host.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Configure an IP packet for tracing.

(IPv4 network)

traceroute [**ip** | **vrf** *vrf-name*] { *hostname* | ipv4-*address* } [**out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | **probe** *probe* | [**source** *interface-type interface-number* | **source** *source-ipv4-address*] | **timeout** *time* | **ttl** *minimum maximum*] *

(IPv6 network)

traceroute [**ipv6** | **vrf** *vrf-name*] { *hostname* | ipv6-*address* } [**out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | **probe** *probe* | [**source** *interface-type interface-number* | **source** *source-ipv6-address*] | **timeout** *time* | **ttl** *minimum maximum*] *

1.6 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

⚠️ **Caution**

Running the **clear** commands may loss vital information and thus interrupt services.

Table 1-1   Monitoring

| Command	Purpose
clear rping table { **all** | **ping-object** *owner-index test-index* | **trace-object** *owner-index test-index* }	Clears the Rping table entries.
show rping detail	Displays detailed information of Rping table entries.

1.7 Configuration Examples

1.7.1 Configuring a Ping Connectivity Test

1.   Requirements

Devices A, B, and C are connected to an IP network. It is required to check whether devices A and C can communicate with each other.

2.   Topology

Figure 1-1   Testing Connectivity with Ping
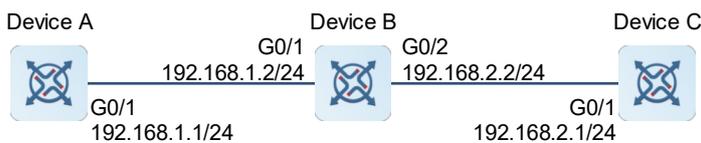
3.   Notes

- Run the following command in privileged mode: **ping** 192.168.2.1.
- Run the following command in privileged mode: **ping** 192.168.2.1, and specify the length of the sent packet, number of sent packets, and TTL.

4.   Procedure

- Use the common Ping function on device A.

    Display the brief Ping result.

```
DeviceA# ping 192.168.2.1
Sending 5, 100-byte ICMP Echoes to 192.168.2.1, timeout is 2 seconds:
```

```
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Display the detailed Ping result.

```
DeviceA# ping 192.168.2.1 detail
Sending 5, 100-byte ICMP Echoes to 192.168.2.1, timeout is 2 seconds:
  < press Ctrl+C to break >
Reply from 192.168.2.1: bytes=100 time=4ms TTL=64
Reply from 192.168.2.1: bytes=100 time=3ms TTL=64
Reply from 192.168.2.1: bytes=100 time=1ms TTL=64
Reply from 192.168.2.1: bytes=100 time=1ms TTL=64
Reply from 192.168.2.1: bytes=100 time=1ms TTL=64


Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms.
```

- Use the extended Ping function on device A.

Display the brief Ping result.

```
DeviceA# ping 192.168.2.1 length 1500 ntimes 100 data ffff source 192.168.1.1
timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.2.1, timeout is 3 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

Display the detailed Ping result.

```
DeviceA# ping 192.168.2.1 length 1500 ntimes 10 data ffff source 192.168.1.1
timeout 3 detail
Sending 20, 1500-byte ICMP Echoes to 192.168.2.1, timeout is 3 seconds:
  < press Ctrl+C to break >
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=2ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64
Reply from 192.168.2.1: bytes=1500 time=1ms TTL=64


Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/3 ms.
```

5. **Verification**

Common Ping function: By default, five 100-byte packets are sent to the specified IP address. Within the specified time (2 seconds by default), the detection information is displayed, and statistical information is output.

Extended Ping function: By default, ten 1500-byte packets are sent to the specified IP address. If there is a response within the specified time (3 seconds), the detection information is displayed, and statistical information is output.
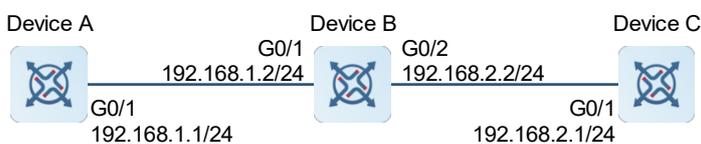
1.7.2 Configuring a Traceroute Connectivity Test

1. Requirements

Devices A, B, and C are connected to an IP network. Device A fails to communicate with device C. It is required to check whether the route between devices A and C is reachable. If the route is unreachable, confirm the faulty network node.

2. Topology

Figure 1-1   Testing connectivity with Traceroute

3. Notes

Run the following command in privileged mode: **traceroute** 192.168.2.1.

4. Procedure

(1) Configure an IP address on devices A, B, and C, respectively. (omitted)

(2) Configure a static route on device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA (config)# ip route 0.0.0.0 0.0.0.0 192.168.1.2
DeviceA (config)# exit
```

(3) Check whether the route between devices A and C is reachable.

```
DeviceA# ping 192.168.2.1
Sending 5, 100-byte ICMP Echoes to 192.168.2.1, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5).
```

(4) Check the faulty network node.

```
DEVICEA# traceroute ip 192.168.2.1
  < press Ctrl+C to break >
Tracing the route to 192.168.2.1
1      192.168.1.2          1 msec  1 msec  1 msec
2      *          *          *
3      *          *          *
4      *          *          *
```

5.   Verification

The displayed result indicates that the route between devices A and C is unreachable. The packet sent from device A to device C has arrived at device B, but a fault occurs to the connection between devices B and C.