Understand the Extended Ping and Extended Traceroute Commands

Contents

Introduction

Prerequisites

- Requirements
- Components Used

The Ping Command

- The Extended Ping Command
- The Ping Command Field Descriptions

The Traceroute Command

- The Extended Traceroute Command
- The Traceroute Command Field Descriptions

Related Information

Introduction

This document describes how to use the extended ping and the extended traceroute commands.

Prerequisites

Requirements

This document requires prior knowledge of the ping and traceroute commands.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS® Software
- All Cisco series routers

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

The Ping Command

The ping (Packet InterNet Groper) command is a very common method to troubleshoot the accessibility of devices. It uses two Internet Control Message Protocol (ICMP) query messages, ICMP echo requests, and ICMP echo replies to determine whether a remote host is active. The ping command also measures the amount of time it takes to receive the echo reply.

The ping command first sends an echo request packet to an address, and then it waits for a reply. The ping is

successful only if the ECHO REQUEST gets to the destination, and the destination is able to get an ECHO REPLY back to the source of the ping within a predefined time interval.

The Extended Ping Command

When a normal ping command is sent from a router, the source address of the ping is the IP address of the interface that the packet uses to exit the router. If an extended ping command is used, the source IP address can be changed to any IP address on the router. The extended ping is used to perform a more advanced check of host reachability and network connectivity. The extended ping command works only at the privileged EXEC command line. The normal ping works both in the user EXEC mode and the privileged EXEC mode. In order to use this feature, enter ping at the command line and press Return. You are prompted for the fields as given in the ping Command Field Descriptions section of this document.

The Ping Command Field Descriptions

This table lists the ping command field descriptions. These fields can be modified with the use of the extended ping command.

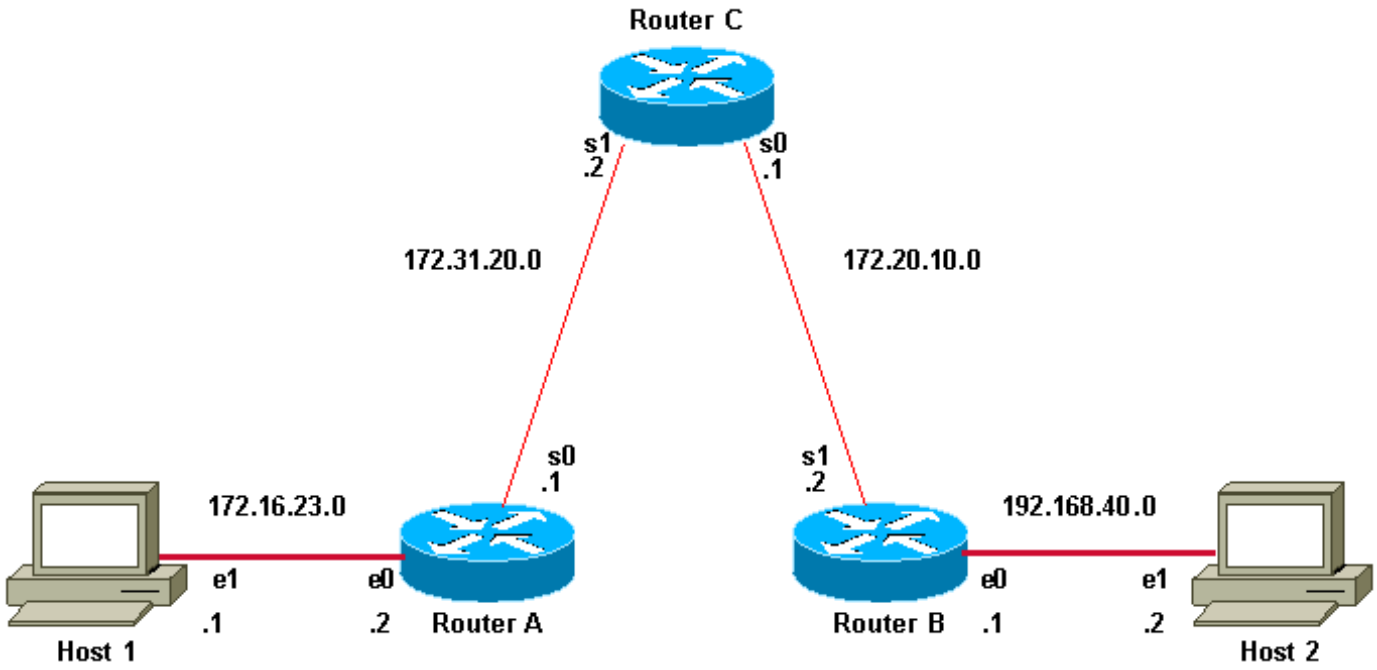
Field	**Description**
Protocol [ip]:	Prompts for a supported protocol. Enter appletalk, clns, ip, novell, apollo, vines, decnet, or xns. The default is ip.
Target IP address:	Prompts for the IP address or host name of the destination node you plan to ping. If you have specified a supported protocol other than IP, enter an appropriate address for that protocol here. The default is none.
Repeat count [5]:	Number of ping packets that are sent to the destination address. The default is 5.
Datagram size [100]:	Size of the ping packet (in bytes). Default: 100 bytes.
Timeout in seconds [2]:	Timeout interval. Default: 2 (seconds). The ping is declared successful only if the ECHO REPLY packet is received before this time interval.
Extended commands [n]:	Specifies whether or not a series of additional commands appears. The default is no.
Ingress ping [n]:	The ingress ping simulates packets received on the specified ingress interface to the target destination. The default is no.

	(The availability of this option differs from the software release used.)
Source address or interface:	The interface or IP address of the router to use as a source address for the probes. The router normally picks the IP address of the outbound interface to use. The interface can also be mentioned, but with the correct syntax as shown here: Source address or interface: ethernet 0 This is a partial output of the extended ping command. The interface cannot be written as e0.
DSCP Value [0]:	Specifies the Differentiated Services Code Point (DSCP). The DSCP value introduced is placed in each probe. The default is 0. (The availability of this option differs from the software release used.)
Type of service [0]:	Specifies the Type of Service (ToS). The requested ToS is placed in each probe, but there is no guarantee that all routers process the ToS. It is the Internet quality of service selection. The default is 0.
Set DF bit in IP header? [no]:	Specifies whether the Don't Fragment (DF) bit is to be set on the ping packet. If yes is specified, the DF option does not allow this packet to be fragmented when it has to go through a segment with a smaller maximum transmission unit (MTU), and you receive an error message from the device that wanted to fragment the packet. This is useful to determine the smallest MTU in the path to a destination. The default is no.
Validate reply data? [no]:	Specifies whether or not to validate the reply data. The default is no.
Data pattern [0xABCD]	Specifies the data pattern. Different data patterns are used to troubleshoot framing errors and clocking problems on serial lines. The default is [0xABCD].
Loose, Strict, Record, Timestamp, Verbose[none]:	IP header options. This prompt offers more than one option to be selected. They are: • Verbose is automatically selected along with any other option.

	• Record is a very useful option because it displays the address(es) of the hops (up to nine) the packet goes through. • Loose allows you to influence the path when you specify the address(es) of the hop(s) you want the packet to go through. • Strict is used to specify the hop(s) that you want the packet to go through, but no other hop(s) are allowed to be visited. • Timestamp is used to measure roundtrip time to particular hosts. The difference between the Record option of this command and the traceroute command is that the Record option not only informs you of the hops that the echo request (ping) went through to get to the destination, but it also informs you of the hops it visited on the return path. With the traceroute command, you do not get information about the path that the echo reply takes. The traceroute command issues prompts for the required fields. The traceroute command places the requested options in each probe. However, there is no guarantee that all routers (or end nodes) process the options. The default is none.
Sweep range of sizes [n]:	Allows you to vary the sizes of the echo packets that are sent. This is used to determine the minimum sizes of the MTUs configured on the nodes along the path to the destination address. Performance problems caused by packet fragmentation is thus reduced. The default is no.
!!!!!	Each exclamation point (!) denotes receipt of a reply. A period (.) denotes that the network server timed out as it waited for a reply. Refer to ping characters for a description of the other characters.
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Any percentage less than 80 is usually considered problematic.
round-trip min/avg/max = 1/2/4 ms	Round-trip travel time intervals for the protocol echo packets with minimum/average/maximum (in milliseconds).

In this diagram, Host 1 and Host 2 are unable to ping each other. You can troubleshoot this problem on the

routers in order to determine if there is a routing problem, or if one of the two hosts do not have their default gateway correctly set.



Host 1 and Host 2 cannot Ping

In order for the ping from Host 1 to Host 2 to succeed, each host needs to point its default gateway to the router on its respective LAN segment, or the host needs to exchange network information with the routers that use a routing protocol. If either host does not have its default gateway set correctly, or it does not have the correct routes in its routing table, it is not able to send packets to destinations that are not present in its Address Resolution Protocol (ARP) cache. It is also possible that the hosts cannot ping each other because one of the routers does not have a route to the subnet from which the host sources its ping packets.

Example

This is an example of the extended **ping** command sourced from the Router A Ethernet 0 interface and destined for the Router B Ethernet interface. If this ping succeeds, it is an indication that there is no routing problem. Router A knows how to get to the Ethernet of Router B, and Router B knows how to get to the Ethernet of Router A. Also, both hosts have their default gateways set correctly.

If the extended ping command from Router A fails, it means that there is a routing problem. There could be a routing problem on any of the three routers. Router A could have lost a route to the subnet of Router B Ethernet, or to the subnet between Router C and Router B. Router B could have lost a route to the subnet of Router A, or to the subnet between Router C and Router A; and Router C could have lost a route to the subnet of Router A or Router B Ethernet segments. You must correct any routing problems, and then Host 1 must try to ping Host 2. If Host 1 still cannot ping Host 2, then you need to check both default gateways. The connectivity between the Ethernet of Router A and the Ethernet of Router B is checked with the extended **ping** command.

With a normal ping from Router A to Router B Ethernet interface, the source address of the ping packet would be the address of the outgoing interface, that is, the address of the serial 0 interface (172.31.20.1). When Router B replies to the ping packet, it replies to the source address (that is, 172.31.20.1). This way, only the connectivity between the serial 0 interface of Router A (172.31.20.1) and the Ethernet interface of Router B (192.168.40.1) is tested.

In order to test the connectivity between Router A Ethernet 0 (172.16.23.2) and Router B Ethernet 0 (192.168.40.1), use the extended ping command. With extended ping, you get the option to specify the source

address of the pingpacket, as shown here:

<#root>

```
RouterA>
```

enable

```
RouterA#
```

ping

```
Protocol [ip]:
Target IP address: 192.168.40.1
```

!--- The address to ping.

```
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.23.2
```

!---Ping packets are sourced from this address.

```
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/97/132 ms
```

!--- Ping is successful.

```
RouterA#
```

This is an example with extended commands and sweep details:

```
RouterA>
```

enable

```
RouterA#
```

ping

```
Protocol [ip]:

!--- The protocol name.



Target IP address: 192.168.40.1

!--- The address to ping.



Repeat count [5]: 10

!--- The number of ping packets that are sent to the destination address.



Datagram size [100]:

!--- The size of the ping packet in size. The default is 100 bytes.



Timeout in seconds [2]:

!--- The timeout interval. The ping is declared successful only if the
!--- ECHO REPLY packet is received before this interval.



Extended commands [n]: y

!--- You choose yes if you want extended command options
!--- (Loose Source Routing, Strict Source Routing, Record route and Timestamp).



Source address or interface: 172.16.23.2

!--- Ping packets are sourced from this address and must be the IP address
!--- or full interface name (for example, Serial0/1 or 172.16.23.2).



Type of service [0]:

!--- Specifies Type of Service (ToS).
```

Set DF bit in IP header? [no]:

!--- Specifies whether or not the Don’t Fragment (DF) bit is to be
!--- set on the ping packet.

Validate reply data? [no]:

!--- Specifies whether or not to validate reply data.

Data pattern [0xABCD]:

!--- Specifies the data pattern in the ping payload. Some physical links
!--- might exhibit data pattern dependent problems. For example, serial links
!--- with misconfigured line coding. Some useful data patterns to test
!--- include all 1s (0Xffff), all 0s (0x0000) and alternating
!--- ones and zeros (0Xaaaa).

Loose, Strict, Record, Timestamp, Verbose[none]:

!--- IP header options.

Sweep range of sizes [n]: y

!--- Choose yes if you want to vary the sizes on echo packets that are sent.

Sweep min size [36]:
Sweep max size [18024]:
Sweep interval [1]:

Sending 179890, [36..18024]-byte ICMP Echos to 192.168.40.1, timeout is 2 seconds:

!--- The count 179890 depends on the values of min sweep,
!--- max sweep, sweep interval and repeat count. Calculations are based on:
!--- 18024(high end of range) - 36(low end of range) = 17988(bytes in range)
!--- 17988(bytes in range) / 1(sweep interval) = 17988 (steps in range)
!--- 17988(bytes in range) + 1 (first value) = 17989(values to be tested)
!--- 17989(values to be tested) * 10(repeat count) = 179890 (pings to be sent)
!--- In order to decrease the value, increase the sweep interval or decrease
!--- the repeat count, or you can even decrease the difference between
!--- Minimum and Maximum sweep size. Based on the previous example, the
!--- number 17890 is an expected value and tries to ping 17890 times.

```
Packet sent with a source address of 172.16.23.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms


!--- Ping is successful.


RouterA#
```

The Traceroute Command

Where ping can be used to verify connectivity between devices, the traceroute command can be used to discover the paths packets take to a remote destination, as well as where routing breaks down.

The purpose behind the traceroute command is to record the source of each ICMP time exceeded message in order to provide a trace of the path the packet took to reach the destination.

The device that executes the traceroute command sends out a sequence of User Datagram Protocol (UDP) datagrams, each with Time-To-Live (TTL) value increments, to an invalid port address (Default 33434) at the remote host.

First, three datagrams are sent, each with a TTL field value set to 1. The TTL value of 1 causes the datagram to timeout as soon as it hits the first router in the path. This router then responds with an ICMP time exceeded message which indicates that the datagram has expired.

Next, three more UDP messages are sent, each with the TTL value set to 2. This causes the second router in the path to the destination to return ICMP time exceeded messages.

This process continues until the packets reach the destination and until the system that originates the traceroute receives ICMP time exceeded messages from every router in the path to the destination. Since these datagrams try to access an invalid port (Default 33434) at the destination host, the host responds with ICMP port unreachable messages that indicate an unreachable port. This event signals the traceroute program to finish.



Note: Make sure you have not disabled the **ip unreachable** command with the **no ip unreachables** under any VLAN. This command makes the packet discard messages without any ICMP error message. In this case, traceroute does not work.

The Extended Traceroute Command

The extended traceroute command is a variation of the traceroute command. An extended **trackers** command can be used to see what path packets take to get to a destination. The command can also be used to check routing at the same time. This is helpful for when you troubleshoot routing loops, or for when you determine where packets are get lost (if a route is gone, or if packets are blocked by an Access Control List or firewall). You can use the extended ping command in order to determine the type of connectivity problem, and then use the extended traceroute command in order to narrow down where the problem occurs.

A time exceeded error message indicates that an intermediate communication server has seen and discarded the packet. A destination unreachable error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, trace prints an asterisk(*).

The command terminates when any of these happens:

- The destination responds.
- The maximum TTL is exceeded.
- The user interrupts the trace with the escape sequence.

 **Note**: You can invoke this escape sequence when you simultaneously press **Ctrl+Shift** and **6**.

The Traceroute Command Field Descriptions

This table lists the traceroute command field descriptions:

Field	**Description**
Protocol [ip]:	Prompts for a supported protocol. Enter appletalk, clns, ip, novell, apollo, vines, decnet, or xns. The default is ip.
Target IP address	You must enter a host name or an IP address. There is no default.
Source address:	The interface or IP address of the router to use as a source address for the probes. The router normally picks the IP address of the outbound interface to use.
Numeric display [n]:	The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display.
Timeout in seconds [3]:	The number of seconds to wait for a response to a probe packet. The default is 3 seconds.

Probe count [3]:	The number of probes to be sent at each TTL level. The default count is 3.
Minimum Time to Live [1]:	The TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.
Maximum Time to Live [30]:	The largest TTL value that can be used. The default is 30. The traceroute command terminates when the destination is reached or when this value is reached.
Port Number [33434]:	The destination port used by the UDP probe messages. The default is 33434.
Loose, Strict, Record, Timestamp, Verbose[none]:	IP header options. You can specify any combination. The traceroute command issues prompts for the required fields. The traceroute command places the requested options in each probe; however, there is no guarantee that all routers (or end nodes) process the options.

Example

<#root>

```
RouterA>
```

enable

```
RouterA#
```

traceroute

```
Protocol [ip]:
Target IP address: 192.168.40.2
```

!--- The address to which the path is traced.

```
Source address: 172.16.23.2
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.40.2
```

```
1 172.31.20.2 16 msec 16 msec 16 msec
2 172.20.10.2 28 msec 28 msec 32 msec
3 192.168.40.2 32 msec 28 msec *

!--- The traceroute is successful.


RouterA#
```



Note: The extended traceroute command can be executed in the privileged EXEC mode only, whereas the normal traceroute command works on both the user and privileged EXEC modes.

Related Information

- TCP/IP Routed Protocols Technology Page
- IP Routing Support Page
- Understand the Ping and Traceroute Commands
- Use the Traceroute Command on Operating Systems
- Cisco Technical Support & Downloads