isco − Using the Extended ping and Extended traceroute Comm

Table of Contents

Using the Extended ping and Extended traceroute Commands

Introduction

This document illustrates how to use the extended **ping** and extended **traceroute** commands. Standard **ping** and **traceroute** commands are covered extensively in the following documents:

- Understanding the **ping** and **traceroute** Commands
- Using the **traceroute** Command on Operating Systems

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

This document requires an understanding of the **ping** and **traceroute** commands which are described in detail in the links given in the Introduction.

Components Used

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

- Cisco IOS® Software Release 12.2(10b)
- All Cisco series routers

The ping Command

The **ping** (Packet InterNet Groper) command is a very common method for troubleshooting 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. To use this feature, enter ping at the command line and press "Return". You are prompted for the following fields as given in the next section.

ping Command Field Descriptions

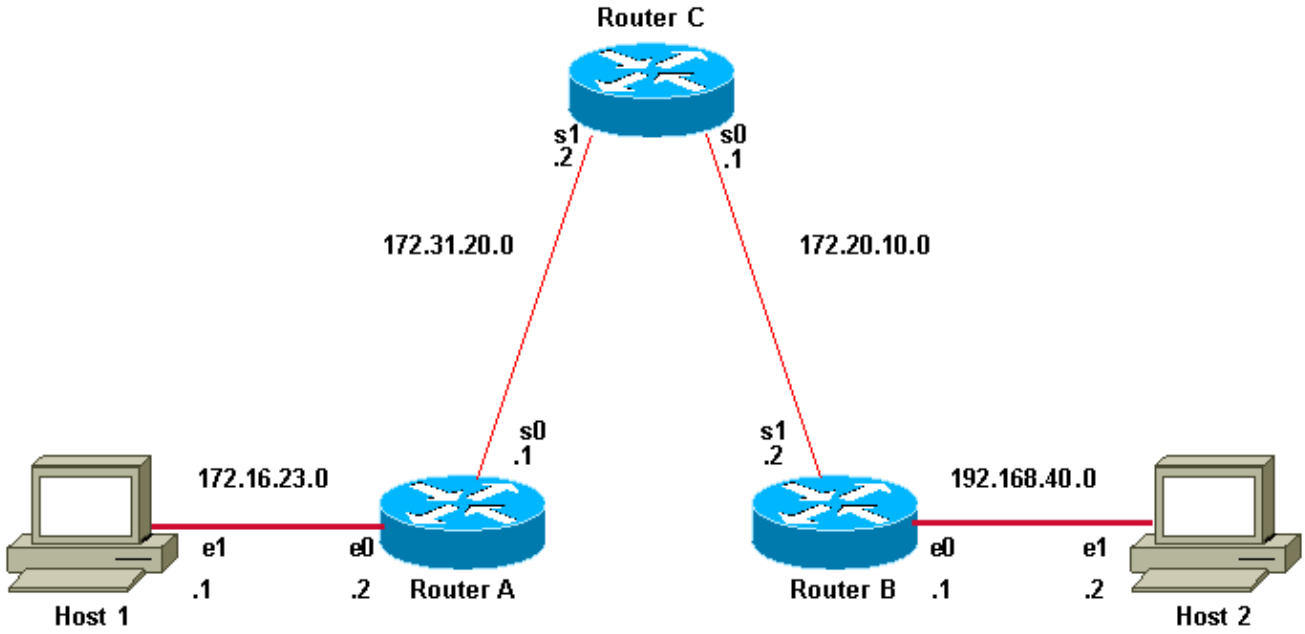
The following table lists the **ping** command field descriptions. As shown in the table below, these fields can be modified with the use of the extended **ping** command.

Field	Description
Protocol [ip]:	Prompts for a supported protocol. Enter appletalk, clns, ip, novell, apollo, vines, decnet, or xns. Default: 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. Default: none.
Repeat count [5]:	Number of ping packets that will be sent to the destination address. Default: 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. Default : no.
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 may also be mentioned, but with the correct syntax as shown below: `Source address or interface: ethernet 0` **Note:** The above is a partial output of the extended **ping** command. The interface cannot

	be written as e0.
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 will process the ToS. It is the Internet service's quality selection. Default : 0.
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. If yes is specified, the Don't Fragment 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 will receive an error message from the device that wanted to fragment the packet. This is useful for determining the smallest MTU in the path to a destination. Default : no.
Validate reply data? [no]:	Specifies whether or not to validate the reply data. Default : no.
Data pattern [0xABCD]	Specifies the data pattern. Different data patterns are used to troubleshoot framing errors and clocking problems on serial lines. Default :[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 by specifying 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 using the **Record** option of this command and using the **traceroute** command is that, the **Record** option of this command 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. Note that the **traceroute** command places the requested options in each probe; however, there is no guarantee that all routers (or end nodes) will process the options. Default : none.
Sweep range of sizes [n]:	Allows you to vary the sizes of the echo packets being 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. Default : no.
!!!!!	Each exclaimation point (!) denotes receipt of a reply. A period (.) denotes that the network server timed out while waiting for a reply. For a description of the remaining characters, refer to ping characters.
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round−trip min/avg/max = 1/2/4 ms	Round−trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

In the diagram below, Host 1 and Host 2 are unable to ping each other. You can troubleshoot this problem on the routers to determine if there is a routing problem, or if one of the two hosts does not have its default gateway correctly set.



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

using 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 will not be able to send packets to destinations 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 is sourcing its ping packets.

Example

Below 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 be missing a route to the subnet of Router B's Ethernet, or to the subnet between Router C and Router B; Router B could be missing a route to the subnet of Router A's subnet, or to the subnet between Router C and Router A; and Router C could be missing a route to the subnet of Router A's or Router B's Ethernet segments. You should correct any routing problems, and then Host 1 should try to ping Host 2. If Host 1 still cannot ping Host 2, then both hosts' default gateways should be checked. The connectivity between the Ethernet of Router A and the Ethernet of Router B is checked with the extended **ping** command as explained below.

With a normal ping from Router A to Router B's 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.

To test the connectivity between Router A's Ethernet 0 (172.16.23.2) and Router B's Ethernet 0 (192.168.40.1), we use the extended ping command. With extended **ping**, we get the option to specify the source address of the **ping** packet, as shown below.

```
Router A>enable
Router A#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 will be 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 162.108.21.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/97/132 ms
```

```
!--- Ping is successful.

Router A#
```

Hence, the above extended **ping** command verifies the IP connectivity between the two IP addresses 172.16.23.2 and 192.168.40.1.

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 to provide a trace of the path the packet took to reach the destination.

The device executing the **traceroute** command sends out a sequence of User Datagram Protocol (UDP) datagrams, each with incrementing Time−To−Live (TTL) values, 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 indicating 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 originating the traceroute has received ICMP "time exceeded" messages from every router in the path to the destination. Since these datagrams are trying to access an invalid port (Default 33434) at the destination host, the host responds with ICMP "port unreachable" messages indicating an unreachable port. This event signals the traceroute program to finish.

The Extended traceroute Command

The extended **traceroute** command is a variation of the **traceroute** command. An extended **traceroute** command can be used to see what path packets are taking to get to a destination. The command can also be used to check routing at the same time. This is helpful for troubleshooting routing loops, or for determining where packets are getting lost (if a route is missing, or if packets are being blocked by an Access Control List (ACL) or firewall). You can use the extended **ping** command to determine the type of connectivity problem, and then use the extended **traceroute** command to narrow down where the problem is occurring.

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 the following happens:

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

Note: The escape sequence can be invoked by simultaneously pressing Ctrl, Shift and "6".

traceroute Command Field Descriptions

The following 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. Default: ip.
Target IP addres	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. Note that the **traceroute** command will place the requested options in each probe; however, there is no guarantee that all routers (or end nodes) will process the options.

Example

```
Router A>enable
Router A#traceroute
Protocol [ip]:
Target IP address: 192.168.40.2
```

```
!--- The address to which the path is being 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 *

!--- Traceroute is successful


Router A#
```

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

Related Information

- **TCP/IP Routing and Routed Protocols Support Page**
- **Technical Support − Cisco Systems**