



# Host Services and Applications Commands on Cisco IOS-XR Software

---

This document describes the commands used to configure and monitor host services and applications such as Domain Name System (DNS), Telnet, File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), and rcp on Cisco IOS-XR software.

# cinetd rate-limit

To configure the rate limit at which service requests are accepted by Cisco inetd (cinetd), use the **cinetd rate-limit** command in global configuration mode. To restore the default, use the **no** form of this command.

**cinetd rate-limit** *value*

**no cinetd rate-limit** *value*

<b>Syntax Description</b>	<i>value</i>	Specifies the number of service requests that are accepted per second. The range is from 1 to 100. The default is 1.
---------------------------	--------------	--

<b>Defaults</b>	The default value is 1.
-----------------	-------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 2.0	This command was introduced.

<b>Usage Guidelines</b>	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the <i>Configuring AAA Services on Cisco IOS-XR Software</i> module of the <i>Cisco IOS-XR System Security Configuration Guide</i> .
-------------------------	---

Any service request that exceeds the rate limit will be rejected. The rate limit is applied to individual applications.

<b>Examples</b>	The following example sets the <b>cinetd rate-limit</b> value to 10:
-----------------	--

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# cinetd rate-limit 10
```

# clear host

To delete temporary entries from the host name-to-address cache, use the **clear host** command in EXEC mode.

```
clear host {host-name | *}
```

Syntax Description		
	<i>host-name</i>	Deletes the entry in the local cache for that host name.
	*	Deletes all entries in the local cache.

**Defaults** No static mapping is configured.

**Command Modes** EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The host name entries are not removed from NVRAM but are cleared in running memory.

Only the temporary entries in the cache are cleared; the permanent entries that were entered with the **domain ipv4 host** or the **domain ipv6 host** commands are not cleared.

**Examples** The following example shows how to clear all temporary entries from the host name-and-address cache:

```
RP/0/RP0/CPU0:router# clear host *
```

Related Commands	Command	Description
	<a href="#">domain ipv4 host</a>	Defines a static IPv4 host name-to-address mapping in the host cache.
	<a href="#">domain ipv6 host</a>	Defines a static IPv6 host name-to-address mapping in the host cache.
	<a href="#">show hosts</a>	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.

# domain ipv4 host

To define a static host name-to-address mapping in the host cache using IPv4, use the **domain ipv4 host** command in global configuration mode. To remove the **domain ipv4 host** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

**domain ipv4 host** *host-name* *v4address1* [*v4address2*...*v4address8*]

**no domain ipv4 host** *host-name* *v4address1*

## Syntax Description

<i>host-name</i>	Name of the host. The first character can be either a letter or a number. If you use a number, the operations you can perform are limited.
<i>v4address1</i>	Associated IP address.
<i>v4address2</i> ... <i>v4address8</i>	(Optional) Additional associated IP address. You can bind up to eight addresses to a host name.

## Defaults

No static mapping is configured.

## Command Modes

Global configuration

## Command History

Release	Modification
Release 2.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The first character can be either a letter or a number. If you use a number, the operations you can perform (such as **ping**) are limited.

## Examples

The following example shows how to define two IPv4 static mappings:

```
RP/0/RP0/CPU0:router(config)# domain ipv4 host host1 192.168.7.18
RP/0/RP0/CPU0:router(config)# domain ipv4 host host2 10.2.0.2 192.168.7.33
```

# domain ipv6 host

To define a static host name-to-address mapping in the host cache using IPv6, use the **domain ipv6 host** command in global configuration mode. To remove the **domain ipv6 host** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

```
domain ipv6 host host-name v6address1 [v6address2...v6address4]
```

```
no domain ipv6 host host-name v6address1
```

## Syntax Description

<i>host-name</i>	Name of the host. The first character can be either a letter or a number. If you use a number, the operations you can perform are limited.
<i>v6address1</i>	Associated IP address.
<i>v6address2...v6address4</i>	(Optional) Additional associated IP address. You can bind up to four addresses to a host name.

## Defaults

No static mapping is configured. IPv4 and IPv6 address prefixes are not enabled.

## Command Modes

Global configuration

## Command History

Release	Modification
Release 2.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The first character can be either a letter or a number. If you use a number, the operations you can perform (such as **ping**) are limited.

## Examples

The following example shows how to define two IPv6 static mappings:

```
RP/0/RP0/CPU0:router(config)# domain ipv6 host host1 192.168.7.18
RP/0/RP0/CPU0:router(config)# domain ipv6 host host2 10.2.0.2 192.168.7.33
```

# domain list

To define a list of default domain names to complete unqualified host names, use the **domain list** command in global configuration mode. To delete a name from a list, use the **no** form of this command.

**domain list** *domain-name*

**no domain list** *domain-name*

## Syntax Description

<i>domain-name</i>	Domain name. Do not include the initial period that separates an unqualified name from the domain name.
--------------------	---

## Defaults

No domain names are defined.

## Command Modes

Global configuration

## Command History

Release	Modification
Release 2.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

If there is no domain list, the domain name that you specified with the **domain name** global configuration command is used to complete unqualified host names. If there is a domain list, the default domain name is not used. The **domain list** command is similar to the **domain name** command, except that you can use the **domain list** command to define a list of domains, each to be tried in turn.

## Examples

The following example shows how to add several domain names to a list:

```
RP/0/RP0/CPU0:router(config)# domain list domain1.com
RP/0/RP0/CPU0:router(config)# domain list domain2.edu
```

The following example adds a name to and then deletes a name from the list:

```
RP/0/RP0/CPU0:router(config)# domain list domain3.edu
RP/0/RP0/CPU0:router(config)# no domain list domain2.edu
```

## Related Commands

Command	Description
<a href="#">domain name</a>	Defines a default domain name to complete unqualified host names.
<a href="#">show hosts</a>	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.

# domain lookup disable

To disable the IP Domain Name System (DNS)-based host name-to-address translation, use the **domain lookup disable** command in global configuration mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

**domain lookup disable**

**no domain lookup disable**

---

**Syntax Description**

This command has no arguments or keywords.

---

**Defaults**

The IP DNS-based host-to-address translation is enabled.

---

**Command Modes**

Global configuration

---

**Command History**

Release	Modification
Release 2.0	This command was introduced.

---

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Using the **no** command removes the specified command from the configuration file and restores the system to its default condition. The **no** form of this command is not stored in the configuration file.

---

**Examples**

The following example shows how to enable the IP DNS-based host name-to-address translation:

```
RP/0/RP0/CPU0:router(config)# domain lookup disable
```

## ■ domain lookup disable

Related Commands	Command	Description
	<a href="#">domain name</a>	Defines a default domain name to complete unqualified host names (names without a dotted decimal domain name).
	<a href="#">domain name-server</a>	Specifies the address of one or more name servers to use for name and address resolution.
	<a href="#">show hosts</a>	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.

# domain name

To define a default domain name that the software uses to complete unqualified host names, use the **domain name** command in global configuration mode. To remove the name, use the **no** form of this command.

**domain name** *domain-name*

**no domain name** *domain-name*

## Syntax Description

<i>domain-name</i>	Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name.
--------------------	---

## Defaults

There is no default domain name.

## Command Modes

Global configuration

## Command History

Release	Modification
Release 2.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

If a host name does not contain a domain name, then a dot and the domain name configured by the **domain name** command are appended to the host name before it is added to the host table.

If no domain name is configured by the **domain name** command and the user provides only the host name, then the request is not looked up.

## Examples

The following example shows how to define cisco.com as the default domain name:

```
RP/0/RP0/CPU0:router(config)# domain name cisco.com
```

## Related Commands

Command	Description
<a href="#">domain list</a>	Defines a list of default domain names to complete unqualified host names.
<a href="#">domain name-server</a>	Specifies the address of one or more name servers to use for name and address resolution.
<a href="#">show hosts</a>	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.

# domain name-server

To specify the address of one or more name servers to use for name and address resolution, use the **domain name-server** command in global configuration mode. To remove the address specified, use the **no** form of this command.

**domain name-server** *server-address*

**no domain name-server** *server-address*

## Syntax Description

<i>server-address</i>	IP addresses of a name server.
-----------------------	--------------------------------

## Defaults

If no name server address is specified, the default name server is 255.255.255.255. IPv4 and IPv6 address prefixes are not enabled.

## Command Modes

Global configuration

## Command History

Release	Modification
Release 2.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

You can enter up to six addresses, but only one per command.

If no name server address is specified, the default name server is 255.255.255.255 so that the DNS lookup can be broadcast to the local network segment. If a DNS server is in the local network, it will reply. If not, there might be a server that knows how to forward the DNS request to the correct DNS server.

## Examples

The following example shows how to specify host 192.168.1.111 as the primary name server and host 192.168.1.2 as the secondary server:

```
RP/0/RP0/CPU0:router(config)# domain name-server 192.168.1.111
RP/0/RP0/CPU0:router(config)# domain name-server 192.168.1.2
```

## Related Commands

Command	Description
<a href="#">domain lookup disable</a>	Enables the IP DNS-based host name-to-address translation.
<a href="#">domain name</a>	Defines a default domain name to complete unqualified host names (names without a dotted decimal domain name).

# ftp client anonymous-password

To assign a password for anonymous users, use the **ftp client anonymous-password** command in global configuration mode. To remove the **ftp client anonymous-password** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

```
ftp client anonymous-password password
```

```
no ftp client anonymous-password
```

---

**Syntax Description**

<i>password</i>	Password for the anonymous user.
-----------------	----------------------------------

---

---

**Command Modes**

Global configuration

---

**Command History**

<b>Release</b>	<b>Modification</b>
Release 2.0	This command was introduced.

---

---

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **ftp client anonymous-password** command is FTP server dependent.

---

**Examples**

The following example shows how to set the anonymous password to xxxx:

```
RP/0/RP0/CPU0:router(config)# ftp client anonymous-password xxxx  
RP/0/RP0/CPU0:router(config)#
```

# ftp client passive

To configure the software to use only passive FTP connections, use the **ftp client passive** command in global configuration mode. To remove the **ftp client passive** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

**ftp client passive**

**no ftp client passive**

**Syntax Description** This command has no arguments or keywords.

**Defaults** FTP data connections are active.

**Command Modes** Global configuration

Command History	Release	Modification
	Release 2.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Using the **ftp client passive** command allows you to make only passive-mode FTP connections. To specify the source IP address for FTP connections, use the **ftp client source-interface** command.

**Examples** The following example shows how to configure the networking device to use only passive FTP connections:

```
RP/0/RP0/CPU0:router(config)# ftp client passive

1d:3h:54:47: ftp_fs[16437]: FTP: verifying tuple passive (SET).
1d:3h:54:47: ftp_fs[16437]: FTP: applying tuple passive (SET).
1d:3h:54:47: ftp_fs[16437]: FTP: passive mode has been enabled.
```

Related Commands	Command	Description
	<a href="#">ftp client source-interface</a>	Specifies the source IP address for FTP connections.

# ftp client source-interface

To specify the source IP address for FTP connections, use the **ftp client source-interface** command in global configuration mode. To remove the **ftp client source-interface** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

**ftp client source-interface** *type instance*

**no ftp client source-interface** *type instance*

Syntax Description	
<i>type</i>	Interface type from which candidate Route Processor (RP) packets will be sourced. For more information, use the question mark (?) online help function.
<i>instance</i>	<p>Either a physical interface instance or a virtual interface instance:</p> <ul style="list-style-type: none"> <li>Physical interface instance. Naming notation is rack/slot/module/port and a slash mark between values is required as part of the notation. <ul style="list-style-type: none"> <li>rack: Chassis number of the rack.</li> <li>slot: Physical slot number of the line card.</li> <li>module: Module number. A Physical Layer Interface Module (PLIM) is always 0.</li> <li>port: Physical port number of the interface.</li> </ul> </li> </ul> <p><b>Note</b> In references to a Management Ethernet interface located on a Route Processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0.</p> <ul style="list-style-type: none"> <li>Virtual interface instance. Number range will vary depending on interface type.</li> </ul> <p>For more information about the syntax for the router, use the question mark (?) online help function.</p>

**Defaults** The FTP source address is the IP address of the interface used by the FTP packets to leave the networking device.

**Command Modes** Global configuration

Command History	Release	Modification
	Release 2.0	This command was introduced.

---

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to set the same source address for all FTP connections. To configure the software to use only passive FTP connections, use the **ftp client passive** command.

---

**Examples**

The following example shows how to configure the IP address associated with POS interface 0/1/2/1 as the source address on all FTP packets, regardless of which interface is actually used to send the packet:

```
RP/0/RP0/CPU0:router (config)# ftp client source-interface POS 0/1/2/1
```

---

**Related Commands**

Command	Description
<a href="#">ftp client passive</a>	Configures the software to use only passive FTP connections.

---

# ping (EXEC)

To check host reachability and network connectivity on IP networks, use the **ping** command in EXEC mode.

```
ping [host-name | ip-address] [count number] [size number] [source {ip-address | type number}]
[timeout seconds] [pattern number] [type number] [priority number] [verbose] [donnotfrag]
[validate] [sweep]
```

Syntax Description	
<i>host-name</i>	(Optional) Host name of the system to ping.
<i>ip-address</i>	(Optional) IP address of the system to ping.
<b>count number</b>	(Optional) Sets the repeat count. Number range is from 0 to 2147483647.
<b>size number</b>	(Optional) Sets the datagram size.
<b>source</b>	(Optional) Identifies the source address or source interface.
<b>type number</b>	(Optional) Sets the type of service from 0 to 255.
<b>timeout seconds</b>	(Optional) Sets the timeout in seconds from 0 to 3600.
<b>priority number</b>	(Optional) Sets the packet priority. The range is from 0 to 15.
<b>pattern number</b>	(Optional) Sets the data pattern. The range is from 0 to 65535.
<b>verbose</b>	(Optional) Sets verbose output.
<b>donnotfrag</b>	(Optional) Sets the Don't Fragment (DF) bit in the IP header.
<b>validate</b>	(Optional) Validates the return packet.
<b>sweep</b>	(Optional) Sets the sweep ping.

**Command Modes** EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The ping program sends an echo request packet to an address and then waits for a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.



**Note** The **ping** (EXEC) command is supported only on IP networks.

If you enter the command without specifying either a host name or IP address, the system prompts you to specify the target IP address and several other command parameters. After specifying the target IP address, you can specify alternate values for the remaining parameters or accept the displayed default for each parameter.

If the system cannot map an address for a host name, it returns an “%Unrecognized host or address, or protocol not running” error message.

To abnormally terminate a ping session, enter the escape sequence—by default, Ctrl-C. Simultaneously press and release the Ctrl and C keys.

Table 1 describes the test characters sent by the ping facility.

**Table 1** ping Test Characters

Character	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
?	Unknown packet type.
U	A “destination unreachable” error PDU was received.
C	A “congestion experienced” packet was received.
M	Fragmentation is needed, but the “don’t fragment” bit in the IP header is set. When this bit is set, the IP layer will not fragment the packet and returns an ICMP error message to the source if the packet size is larger than the maximum transmission size. When this bit is not set, the IP layer fragments the packet in order to forward it to the next hop.
Q	A source quench packet was received.



**Note** Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and are answered only by another Cisco networking device.

## Examples

If you do not enter a host name or address on the same line as the **ping** command, the system prompts you to specify the target IP address and several other command parameters. After specifying the target IP address, you can specify alternate values for the remaining parameters or accept the displayed default for each parameter. Although the precise dialog varies somewhat from protocol to protocol, all are similar to the ping session, using default values shown in the following output:

```
RP/0/RP0/CPU0:router# ping

Protocol [ip]:
Target IP address: 10.0.0.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]: yes
Source address or interface: 10.0.0.2
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]: yes
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.25.58.21, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/11/49 ms
```

If you enter a host name or address on the same line as the **ping** command, the command performs the default actions appropriate for the protocol type of that host name or address, as shown in the following output:

```
RP/0/RP0/CPU0:router# ping server01
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/9 ms
```

# rcp client source-interface

To specify the source IP address for remote copy protocol (rcp) connections, use the **rcp client source-interface** command in global configuration mode. To remove the **rcp client source-interface** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

**rcp client source-interface** *type instance*

**no rcp client source-interface** *type instance*

Syntax Description	<i>type</i>	Interface type from which candidate RP packets will be sourced. For more information, use the question mark (?) online help function.
	<i>instance</i>	<p>Either a physical interface instance or a virtual interface instance:</p> <ul style="list-style-type: none"> <li>Physical interface instance. Naming notation is rack/slot/module/port and a slash mark between values is required as part of the notation. <ul style="list-style-type: none"> <li>rack: Chassis number of the rack.</li> <li>slot: Physical slot number of the line card.</li> <li>module: Module number. A Physical Layer Interface Module (PLIM) is always 0.</li> <li>port: Physical port number of the interface.</li> </ul> </li> </ul> <p><b>Note</b> In references to a Management Ethernet interface located on a Route Processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0.</p> <ul style="list-style-type: none"> <li>Virtual interface instance. Number range will vary depending on interface type.</li> </ul> <p>For more information about the syntax for the router, use the question mark (?) online help function.</p>

**Defaults** The rcp source address is the IP address of the interface used by the rcp packets to leave the networking device.

**Command Modes** Global configuration

Command History	Release	Modification
	Release 2.0	This command was introduced.

---

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to set the IP address of an interface as the source for all rcp connections. To configure the remote username to be used when a remote copy using rcp is requested, use the **rcp client username** command.

---

**Examples**

The following example shows how to set the IP address for POS interface 1/0/2/1 as the source address for rcp connections:

```
RP/0/RP0/CPU0:router(config)# rcp client source-interface POS 1/0/2/1
```

---

**Related Commands**

Command	Description
<a href="#">rcp client username</a>	Configures the remote username to be used when a remote copy using rcp is requested.

---

# rcp client username

To configure the local user on the client side to be used when requesting a remote copy using Remote Copy Protocol (rcp), use the **rcp client username** command in global configuration mode. To restore the system to its default condition, use the **no** form of this command.

**rcp client username** *username*

**no rcp client username** *username*

## Syntax Description

<i>username</i>	Name of the remote user on the rcp server. This name is used for rcp copy requests. All files and images to be copied are searched for or written relative to the directory of the remote user's account if the rcp server has a directory structure, as do UNIX systems.
-----------------	---

## Defaults

If you do not issue this command, the software sends the remote username associated with the current tty process, if that name is valid, for rcp copy commands. For example, if the user is connected to the networking device through Telnet and the user was authenticated through the **username** command, the software sends that username as the remote username.

If the username for the current tty process is not valid, the software sends the host name as the remote username. For rcp boot commands, the software sends the network server host name by default.



**Note** For Cisco, tty lines are commonly used for access services. The concept of tty originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are called tty devices (tty stands for teletype, the original UNIX terminal).

## Command Modes

Global configuration

## Command History

Release	Modification
Release 2.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The rcp protocol requires that a client send the remote username on an rcp request to the network server. Use this command to specify the remote username to be sent to the network server for an rcp copy request. If the network server has a directory structure, as do UNIX systems, all files and images to be copied are searched for or written relative to the directory of the remote user's account. To specify a source address for rcp connections, use the **rcp client source-interface** command.



### Caution

The remote username must be associated with an account on the destination server.

---

**Examples**

The following example shows how to configure the remote username to netadmin1:

```
RP/0/RP0/CPU0:router(config)# rcp client username netadmin1
```

---

**Related Commands**

Command	Description
<a href="#">rcp client source-interface</a>	Specifies the source IP address for rcp connections.

---

# show cinetd services

To display the services whose processes are spawned by cinetd when a request is received, use the **show cinetd services** command in EXEC mode.

**show cinetd services**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

**Examples** The following example is output from the **show cinetd services** command:

```
RP/0/RP0/CPU0:router# show cinetd services
```

```
Family Service  Proto  Port  ACL  max_cnt  curr_cnt  wait  Program Option
=====
v4    telnet   tcp    23   unlimited  0        nowait  telnet
v4    tftp     udp    69   unlimited  0        wait    tftpd  disk0
```

Related Commands	Command	Description
	<b>telnet ipv4 server</b>	Enables Telnet services on a networking device.
	<b>tftp ipv4 server</b>	Enables or disables the TFTP server or a feature running on the TFTP server.

# show hosts

To display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses, use the **show hosts** command in EXEC mode.

**show hosts** [*host-name*]

<b>Syntax Description</b>	<i>host-name</i>	(Optional) Name of the host about which to display information. If omitted, all entries in the local cache are displayed.
---------------------------	------------------	---

**Defaults** Unicast address prefixes are the default when IPv4 address prefixes are configured.

**Command Modes** EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 2.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

**Examples** The following is sample output from the **show hosts** command:

```
RP/0/RP0/CPU0:router# show hosts

Default domain is cisco.com
Name/address lookup uses domain service
Name servers are 255.255.255.255
Host          Flags          Age(hr)   Type          Address(es)
host1.cisco.com (temp, OK)    1         IP            192.168.4.10
abc           (perm, OK)    0         IP            10.0.0.0 10.0.0.2 10.0.0.3
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">clear host</a>	Deletes entries from the host-name-and-address cache.
	<a href="#">domain list</a>	Defines a list of default domain names to complete unqualified host names.
	<a href="#">domain lookup disable</a>	Enables the IP DNS-based host name-to-address translation.
	<a href="#">domain name</a>	Defines a default domain name to complete unqualified host names (names without a dotted-decimal domain name).
	<a href="#">domain name-server</a>	Specifies the address of one or more name servers to use for name and address resolution.

# telnet

To log in to a host that supports Telnet, use the **telnet** command in EXEC mode.

```
telnet {ip-address | host-name} [options]
```

## Syntax Description

<i>ip-address</i>	IP address of a specific host on a network.
<i>host-name</i>	Name of a specific host on a network.
<i>options</i>	(Optional) Telnet connection options. See <a href="#">Table 2</a> for a list of supported options.

## Defaults

Telnet client is in telnet connection options nostream mode.

## Command Modes

EXEC

## Command History

Release	Modification
Release 2.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

If the Telnet server is enabled, you should be able to start a telnet session as long as you have a valid username and password.

[Table 2](#) lists the supported Telnet connection options.

**Table 2** Telnet Connection Options

Option	Description
<i>/stream</i>	Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UUCP and other non-Telnet protocols.
<i>/nostream</i>	Turns off stream processing.
<i>port number</i>	Port number. The range is from 0 to 65535
<i>/source-interface</i>	Specify source interface.

To display a list of the available hosts, use the **show hosts** command. To display the status of all TCP connections, use the **show tcp** command.

The software assigns a logical name to each connection, and several commands use these names to identify connections. The logical name is the same as the host name, unless that name is already in use or you change the connection name with the **name-connection EXEC** command. If the name is already in use, the software assigns a null name to the connection.

The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is Ctrl-^ (press and hold the Control and Shift keys and the 6 key). You can enter the command character as you hold down Ctrl or with Ctrl released; you can use either uppercase or lowercase letters. [Table 3](#) lists the special Telnet escape sequences.

**Table 3 Special Telnet Escape Sequences**

Escape Sequence <sup>1</sup>	Purpose
Ctrl-^ c	Interrupt Process (IP).
Ctrl-^ o	Abort Output (AO).
Ctrl-^ u	Erase Line (EL).

1. The caret (^) symbol refers to Shift-6 on your keyboard.

At any time during an active Telnet session, you can list the Telnet commands by pressing the escape sequence keys followed by a question mark at the system prompt:

**Ctrl-^ ?**

A sample of this list follows. In this sample output, the first caret (^) symbol represents the Control key, and the second caret represents Shift-6 on your keyboard:

```
RP/0/RP0/CPU0:router# ^^?
[Special telnet escape help]
^^B sends telnet BREAK
^^C sends telnet IP
^^H sends telnet EC
^^O sends telnet AO
^^T sends telnet AYT
^^U sends telnet EL
```

You can have several concurrent Telnet sessions open and switch among them. To open a subsequent session, first suspend the current connection by pressing the escape sequence (Ctrl-Shift-6 and then x [Ctrl^x] by default) to return to the system command prompt. Then open a new connection with the **telnet** command.

To terminate an active Telnet session, issue any of the following commands at the prompt of the device to which you are connecting:

- **close**
- **disconnect**
- **exit**
- **logout**
- **quit**

---

**Examples**

The following example shows how to establish a Telnet session to a remote host named host1:

```
RP/0/RP0/CPU0:router# telnet host1
```

---

**Related Commands**

Command	Description
<b>aaa authentication login default local</b>	Sets AAA authentication at login.
<b>telnet server</b>	Enables Telnet services on a networking device.
<b>terminal length</b>	Sets the number of lines on the current terminal screen for the current session.
<b>terminal width</b>	Sets the number of character columns on the terminal screen for the current session.

# telnet server

To enable Telnet services on a networking device, use the **telnet server** command in global configuration mode. To disable Telnet services, use the **no** form of this command.

```
telnet {ipv4 | ipv6} server {access-list name | disable | enable | max-servers}
```

```
no telnet {ipv4 | ipv6} server {access-list name | disable | enable | max-servers}
```

## Syntax Description

<b>access-list</b> <i>name</i>	Specifies an access list by name.
<b>disable</b>	Disables Telnet servers.
<b>enable</b>	Enables Telnet servers.
<b>max-servers</b>	Sets the number of allowable Telnet servers.

## Defaults

Telnet services are disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
Release 2.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Disable Telnet services to prevent inbound Telnet connections from being accepted into a networking device using the **telnet** command. After Telnet services are disabled, no new inbound connections will be accepted, and the Cisco Internet services daemon (cinetd) will stop listening on the Telnet port.

Enable Telnet services to allow inbound Telnet connections into a networking device.

This command affects only inbound Telnet connections to a networking device. Outgoing Telnet connections can be made regardless of whether Telnet services are enabled.

Using the **no** form of the command removes the specified command from the configuration file and restores the system to its default condition with respect to the command. We recommend that you use the **disable** keyword rather than the **no** form of the command to disable the functionality of the command. The **no** form of the command is not stored in the configuration file. Instead, the command with the **disable** keyword is stored in the configuration file.

## Examples

The following example shows how to disable Telnet services on a networking device:

```
RP/0/RP0/CPU0:router(config)# telnet server disable
```

telnet server

**Related Commands**

Command	Description
<a href="#">telnet</a>	Logs in to a host that supports Telnet.

# telnet transparent

To send a CR (carriage return) as a CR-NULL rather than a CR-LF (carriage return-line feed) for virtual terminal sessions, use the **telnet transparent** command in line vty configuration mode. To remove the **telnet transparent** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

**telnet transparent**

**no telnet transparent**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Line template configuration

Command History	Release	Modification
	Release 2.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This command is useful for coping with different interpretations of end-of-line handling in the Telnet protocol specification.

**Examples** The following example shows how to configure the vty line to operate in Telnet transparent mode, wherein any carriage return key is sent as a CR-NULL key combination rather than a CR-LF key combination:

```
RP/0/RP0/CPU0:router(config)# line vty
RP/0/RP0/CPU0:router(line-vty-config)# telnet transparent
```

Related Commands	Command	Description
	<a href="#">telnet</a>	Logs in to a host that supports Telnet.

# tftp client source-interface

To specify the source IP address for a TFTP connection, use the **tftp client source-interface** command in global configuration mode. To remove the **tftp client source-interface** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

**tftp client source-interface** *type instance*

**no tftp client source-interface** *type instance*

Syntax Description		
	<i>type</i>	Interface type from which candidate Route Processor (RP) packets will be sourced. For more information, use the question mark (?) online help function.
	<i>instance</i>	<p>Either a physical interface instance or a virtual interface instance:</p> <ul style="list-style-type: none"> <li>Physical interface instance. Naming notation is rack/slot/module/port and a slash mark between values is required as part of the notation. <ul style="list-style-type: none"> <li>rack: Chassis number of the rack.</li> <li>slot: Physical slot number of the line card.</li> <li>module: Module number. A Physical Layer Interface Module (PLIM) is always 0.</li> <li>port: Physical port number of the interface.</li> </ul> </li> </ul> <p><b>Note</b> In references to a Management Ethernet interface located on a Route Processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0.</p> <ul style="list-style-type: none"> <li>Virtual interface instance. Number range will vary depending on interface type.</li> </ul> <p>For more information about the syntax for the router, use the question mark (?) online help function.</p>

**Defaults** The IP address of the best route to the destination will be used as the source IP address.

**Command Modes** Global configuration

Command History	Release	Modification
	Release 2.0	This command was introduced.

---

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to set the IP address of an interface as the source for all TFTP connections.

---

**Examples**

The following example shows how to set the IP address for POS interface 1/0/2/1 as the source address for TFTP connections:

```
RP/0/RP0/CPU0:router(config)# tftp client source-interface POS 1/0/2/1
```

---

**Related Commands**

Command	Description
<a href="#">tftp server</a>	Enables the TFTP server to start or stop listening for TFTP connections.

---

# tftp server

To enable or disable the TFTP server or a feature running on the TFTP server, use the **tftp server** command in global configuration mode. To restore the system to its default condition, use the **no** form of this command.

```
tftp {ipv4 | ipv6} server [access-list name] {homedir tftp-home-directory} [max-servers number]
```

```
no tftp {ipv4 | ipv6} server [access-list name] {homedir tftp-home-directory} [max-servers number]
```

## Syntax Description

<b>ipv4</b>	Specifies IPv4 address prefixes.
<b>ipv6</b>	Specifies IPv6 address prefixes.
<b>access-list</b> <i>name</i>	(Optional) Specifies the name of the access list associated with the TFTP server.
<b>homedir</b> <i>tftp-home-directory</i>	Specifies the home directory.
<b>max-servers</b> <i>number</i>	(Optional) Sets the maximum number of concurrent TFTP servers. The range is from 1 to 2147483647.

## Defaults

The TFTP server is disabled by default.

## Command Modes

Global configuration

## Command History

Release	Modification
Release 2.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Using the **no** form of this command removes the specified command from the configuration file and restores the system to its default condition. The **no** form of the command is not stored in the configuration file.

## Examples

The following example shows the TFTP server is enabled for the access list named test:

```
RP/0/RP0/CPU0:router(config)# tftp ipv4 server access-list test homedir disk0
```

## Related Commands

Command	Description
<a href="#">show cinetd services</a>	Ensures that the TFTP server is enabled correctly.

# traceroute ipv4

To discover the routes that packets will actually take when traveling to their destination across an IP network, use the **traceroute ipv4** command in EXEC mode.

```
traceroute [host-name | ip-address] [source ip-address-name] [numeric] [timeout seconds]
           [probe count] [minttl seconds] [maxttl seconds] [port number] [priority number] [verbose]
```

Syntax Description	
<i>host-name</i>	(Optional) Host name of system to use as the destination of the trace attempt.
<i>ip-address</i>	(Optional) Address of system to use as the destination of the trace attempt.
<b>source</b>	(Optional) Source address.
<i>ip-address-name</i>	(Optional) IP address A.B.C.D or host name.
<b>numeric</b>	(Optional) Numeric display only.
<b>timeout</b> <i>seconds</i>	(Optional) Timeout value. Range is from 0 to 3600.
<b>probe</b> <i>count</i>	(Optional) Probe count. Range is from 0 to 65535.
<b>minttl</b> <i>seconds</i>	(Optional) Minimum time to live. Range is from 0 to 255.
<b>maxttl</b> <i>seconds</i>	(Optional) Maximum time to live. Range is from 0 to 255.
<b>port</b> <i>number</i>	(Optional) Port number. Range is from 0 to 65535.
<b>priority</b> <i>number</i>	(Optional) Packet priority. Range is from 0 to 15.
<b>verbose</b>	(Optional) Verbose output.

**Command Modes** EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **traceroute ipv4** command works by taking advantage of the error messages generated by networking devices when a datagram exceeds its time-to-live (TTL) value.

The **traceroute ipv4** command starts by sending probe datagrams with a TTL value of 1, which causes the first networking device to discard the probe datagram and send back an error message. The **traceroute ipv4** command sends several probes at each TTL level and displays the round-trip time for each.

The **traceroute ipv4** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A “time exceeded” error message indicates that an intermediate networking device has seen and discarded the probe. 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, **traceroute ipv4** prints an asterisk (\*).

The **tracert** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence, which is, by default, Ctrl-C. Simultaneously press and release the Ctrl and C keys.

To use nondefault parameters and invoke an extended **tracert** test, enter the command without a *host-name* or *ip-address* argument. You will be stepped through a dialog to select the desired parameter values for the **tracert** test.

### Common Trace Problems

Because of how IP is implemented on various networking devices, the IP **tracert** command may behave in unexpected ways.

Not all destinations will respond correctly to a probe message by sending back an “ICMP port unreachable” message. A long sequence of TTL levels with only asterisks, terminating only when the maximum TTL has been reached, may indicate this problem.

There is a known problem with the way some hosts handle an “ICMP TTL exceeded” message. Some hosts generate an “ICMP” message, but they reuse the TTL of the incoming packet. Because this value is zero, the ICMP packets do not succeed in returning. When you trace the path to such a host, you may see a set of TTL values with asterisks (\*). Eventually the TTL is raised high enough that the “ICMP” message can get back. For example, if the host is six hops away, **tracert** will time out on responses 6 through 11.

### Examples

The following display shows a sample **tracert** session when a destination host name has been specified:

```
RP/0/RP0/CPU0:router# tracert host8-sun

Type escape sequence to abort.
Tracing the route to 192.168.0.73
 1 192.168.1.6 (192.168.1.6) 10 msec 0 msec 10 msec
 2 gateway01-gw.gateway.cisco.com (192.168.16.2) 0 msec 10 msec 0 msec
 3 host8-sun.cisco.com (192.168.0.73) 10 msec * 0 msec
```

The following display shows a sample extended **tracert** session when a destination host name is not specified:

```
RP/0/RP0/CPU0:router# tracert
Protocol [ip]:
Target IP address: ena-view3
Source address: 10.0.58.29
Numeric display? [no]:
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 171.71.164.199

 1 sjc-jpollack-vpn.cisco.com (10.25.0.1) 30 msec 4 msec 4 msec
 2 15lab-vlan525-gw1.cisco.com (172.19.72.2) 7 msec 5 msec 5 msec
 3 sjc15-00lab-gw1.cisco.com (172.24.114.33) 5 msec 6 msec 6 msec
 4 sjc5-lab4-gw1.cisco.com (172.24.114.89) 5 msec 5 msec 5 msec
 5 sjc5-sbb4-gw1.cisco.com (171.71.241.162) 5 msec 6 msec 6 msec
 6 sjc5-dc5-gw1.cisco.com (171.71.241.10) 6 msec 6 msec 5 msec
 7 sjc5-dc1-gw1.cisco.com (171.71.243.2) 7 msec 8 msec 8 msec
```

```
8 ena-view3.cisco.com (171.71.164.199) 6 msec * 8 msec
```

Table 4 describes the characters that can appear in traceroute output.

**Table 4** *traceroute Text Characters*

Character	Description
xx msec	For each node, the round-trip time in milliseconds for the specified number of probes.
*	The probe has timed out.
?	Unknown packet type.
A	Administratively unreachable. This output usually indicates that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
U	Port unreachable.

#### Related Commands

Command	Description
<a href="#">traceroute ipv6</a>	Discovers the routes that packets will actually take when traveling to their destination across an IPv6 network.

# tracertoute ipv6

To discover the routes that packets will actually take when traveling to their destination across an IPv6 network, use the **tracertoute ipv6** command in EXEC mode.

```
tracertoute ipv6 [host-name | ip-address] [source ip-address-name] [numeric] [timeout seconds]
[probe count] [minttl seconds] [maxttl seconds] [port number] [priority number] [verbose]
```

## Syntax Description

<i>host-name</i>	(Optional) Host name of system to use as the destination of the trace attempt.
<i>ip-address</i>	(Optional) IPv6 address of system to use as the destination of the trace attempt.
<b>source</b>	(Optional) Source address.
<i>ip-address-name</i>	(Optional) IP address A.B.C.D or host name.
<b>numeric</b>	(Optional) Numeric display only.
<b>timeout</b> <i>seconds</i>	(Optional) Timeout value. Range is from 0 to 3600.
<b>probe</b> <i>count</i>	(Optional) Probe count. Range is from 0 to 65535.
<b>minttl</b> <i>seconds</i>	(Optional) Minimum time to live. Range is from 0 to 255.
<b>maxttl</b> <i>seconds</i>	(Optional) Maximum time to live. Range is from 0 to 255.
<b>port</b> <i>number</i>	(Optional) Port number. Range is from 0 to 65535.
<b>priority</b> <i>number</i>	(Optional) Packet priority. Range is from 0 to 15.
<b>verbose</b>	(Optional) Verbose output.

## Command Modes

EXEC

## Command History

Release	Modification
Release 2.0	This command was introduced.

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **tracertoute ipv6** command works by taking advantage of the error messages generated by networking devices when a datagram exceeds its time-to-live (TTL) value.

The **tracertoute ipv6** command starts by sending probe datagrams with a TTL value of 1, which causes the first networking device to discard the probe datagram and send back an error message. The **tracertoute** command sends several probes at each TTL level and displays the round-trip time for each.

The **tracertoute ipv6** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A “time exceeded” error message indicates that an intermediate networking device has seen and discarded the probe. 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, **tracertoute ipv6** prints an asterisk (\*).

The **traceroute ipv6** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence, which is, by default, Ctrl-C. Simultaneously press and release the Ctrl and C keys.

To use nondefault parameters and invoke an extended **traceroute ipv6** test, enter the command without a *host-name* or *ip-address* argument. You will be stepped through a dialog to select the desired parameter values for the **traceroute ipv6** test.

### Common Trace Problems

Because of how IP is implemented on various networking devices, the IP **traceroute ipv6** command may behave in unexpected ways.

Not all destinations will respond correctly to a probe message by sending back an “ICMP port unreachable” message. A long sequence of TTL levels with only asterisks, terminating only when the maximum TTL has been reached, may indicate this problem.

There is a known problem with the way some hosts handle an “ICMP TTL exceeded” message. Some hosts generate an “ICMP” message, but they reuse the TTL of the incoming packet. Because this value is zero, the ICMP packets do not succeed in returning. When you trace the path to such a host, you may see a set of TTL values with asterisks (\*). Eventually the TTL is raised high enough that the “ICMP” message can get back. For example, if the host is six hops away, **traceroute ipv6** will time out on responses 6 through 11.

### Examples

The following display shows a sample **traceroute ipv6** session when a destination host name has been specified:

```
RP/0/RP0/CPU0:router# traceroute ipv6 host8-sun

Type escape sequence to abort.
Tracing the route to 192.168.0.73
 1 192.168.1.6 (192.168.1.6) 10 msec 0 msec 10 msec
 2 gateway01-gw.gateway.cisco.com (192.168.16.2) 0 msec 10 msec 0 msec
 3 host8-sun.cisco.com (192.168.0.73) 10 msec * 0 msec
```

The following display shows a sample extended **traceroute ipv6** session when a destination host name is not specified:

```
RP/0/RP0/CPU0:router# traceroute ipv6
Target IP address: host8-sun
Source address:
Numeric display? [no]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:

Type escape sequence to abort.
Tracing the route to 192.168.0.73
 1 192.168.1.6 (192.168.1.6) 10 msec 0 msec 10 msec
 2 gateway01-gw.gateway.cisco.com (192.168.16.2) 0 msec 10 msec 0 msec
 3 lab01-lab.cisco.com (192.168.112.57) 10 msec 10 msec 0 msec
 4 lab02-lab.cisco.com (192.168.4.17) 10 msec 10 msec 0 msec
 5 lab03-lab.cisco.com (192.168.14.169) 10 msec 0 msec 0 msec
 6 host8-sun.cisco.com (192.168.0.73) 10 msec * 0 msec
```

Table 5 describes the characters that can appear in **tracertoute ipv6** output.

**Table 5** *tracertoute ipv6* Text Characters

Character	Description
xx msec	For each node, the round-trip time in milliseconds for the specified number of probes.
*	The probe has timed out.
?	Unknown packet type.
A	Administratively unreachable. This output usually indicates that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
U	Port unreachable.

#### Related Commands

Command	Description
<a href="#">tracertoute ipv4</a>	Probes the routes that packets follow when traveling to their destination from the networking device.