

Host Services and Applications Commands

This chapter describes the commands used to configure and monitor the Host Services and Applications on Cisco 8000 Series Routers.

For detailed information about Host Services and Applications concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco 8000 Series Routers*.

- cinetd rate-limit, on page 3
- clear host, on page 4
- domain ipv4 host, on page 5
- domain ipv6 host, on page 6
- domain list, on page 7
- domain lookup disable, on page 8
- domain name (IPAddr), on page 9
- domain name-server, on page 10
- ftp client anonymous-password, on page 11
- ftp client passive, on page 12
- ftp client password, on page 13
- ftp client source-interface, on page 14
- ftp client username, on page 16
- http client connection, on page 17
- http client response, on page 18
- http client secure-verify-host, on page 19
- http client secure-verify-peer, on page 20
- http client source-interface, on page 21
- http client ssl, on page 22
- http client tcp-window-scale, on page 23
- http client version, on page 24
- http client vrf, on page 25
- icmp ipv4 mpls extended-diagnostics, on page 26
- icmp ipv4 vrf extended-diagnostics permitted-remote-address, on page 27
- icmp ipv6 mpls extended-diagnostics, on page 28
- icmp ipv6 vrf extended-diagnostics permitted-remote-address, on page 29
- logging source-interface vrf, on page 30
- ping bulk (network), on page 31
- ping (network), on page 33

- probe, on page 36
- scp, on page 38
- show cinetd services, on page 40
- show hosts, on page 42
- telnet, on page 44
- telnet client source-interface, on page 47
- telnet dscp, on page 49
- telnet server, on page 51
- telnet transparent, on page 53
- tftp server, on page 54
- tftp client source-interface, on page 56
- traceroute, on page 57

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 XR Config mode. To restore the default, use the **no** form of this command.

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

Syntax Description

value	Number of service requests that are accepted per second. Range is 1 to 100. Default is 1.

Command Default

One service request per second is accepted.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows the **cinetd rate-limit** being set to 10:

```
Router# config
Router(config)# cinetd rate-limit 10
```

clear host

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

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

Syntax Description

host-name	Name of host to be deleted.
*	Specifies that all entries in the local cache be deleted.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The dynamic host entries in the cache are cleared.

The temporary entries in the cache are cleared; the permanent entries that were entered with the `domain ipv4 host` or the `domain ipv6 host` command are not cleared.

By default, no static mapping is configured.

Task ID

Task ID	Operations
ip-services	execute

Examples

The following example shows how to clear all temporary entries from the hostname-and-address cache:

```
Router# clear host *
```

domain ipv4 host

To define a static hostname-to-address mapping in the host cache using IPv4, use the **domain ipv4 host** command in XR Config 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 v4address2.....v4address8*
no domain ipv4 host *host-name v4address1*

Syntax Description

host-name	Name of the host. The first character can be either a letter or a number.
v4address1	Associated IP address.
v4address2...v4address8	(Optional) Additional associated IP address. You can bind up to eight addresses to a hostname.

Command Default

No static mapping is configured.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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.

Task ID

Task ID	Operations
ip-services	read, write
basic-services	read, write

Examples

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

```
Router(config)# domain ipv4 host host1 192.168.7.18
Router(config)# domain ipv4 host bost2 10.2.0.2 192.168.7.33
```

domain ipv6 host

To define a static hostname-to-address mapping in the host cache using IPv6, use the **domain ipv6 host** command in XR Config 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

host-name	Name of the host. The first character can be either a letter or a number.
v6address1	Associated IP address.
v6address2...v6address4	(Optional) Additional associated IP address. You can bind up to four addresses to a hostname.

Command Default

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

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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.

Task ID

Task ID	Operations
ip services	read, write

Examples

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

```
Router(config)# domain ipv6 host host1 ff02::2
Router(config)# domain ipv6 host host2 ff02::1
```

domain list

To define a list of default domain names to complete unqualified hostnames, use the **domain list** command in XR Config 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

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

Command Default

No domain names are defined.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ip-service	read, write

Examples

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

```
Router(config)# domain list domain1.com
Router(config)# domain list domain2.edu
```

The following example shows how to add a name to and then delete a name from the list:

```
Router(config)# domain list domain3.edu
Router(config)# no domain list domain2.edu
```

domain lookup disable

To disable the IP Domain Name System (DNS)-based hostname-to-address translation, use the **domain lookup disable** command in XR Config 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 keywords or arguments.

Command Default

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

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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.

Task ID

Task ID	Operations
ip-services	read, write

Examples

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

```
Router(config)# domain lookup disable
```

domain name (IPAddr)

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

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

Syntax Description

domain-name	Default domain name used to complete unqualified hostnames. Do not include the initial period that separates an unqualified name from the domain name.

Command Default

There is no default domain name.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If a hostname does not contain a domain name, then a dot and the domain name configured by the **domain name** command are appended to the hostname 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 hostname, then the request is not looked up.

Task ID

Task ID	Operations
ip-services	read, write

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 XR Config 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

server-address	IP address of a name server.

Command Default

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

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

You can enter up to six addresses, but only one for each 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 replies. If not, there might be a server that knows how to forward the DNS request to the correct DNS server.

Task ID

Task ID	Operations
ip-services	read, write

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:

```
Router(config)# domain name-server 192.168.1.111
Router(config)# domain name-server 192.168.1.2
```

ftp client anonymous-password

To assign a password for anonymous users, use the **ftp client anonymous-password** command in XR Config 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

password	Password for the anonymous user.

Command Default

No default behavior or values

Command Modes

XR Config mode

Command History

Release	Modification
Release 25.4.1	The **ftp** keyword is deprecated.
Release 7.0.12	This command was introduced.

Usage Guidelines

The **ftp client anonymous-password** command is File Transfer Protocol (FTP) server dependent.

Starting with Cisco IOS XR Software Release 25.4.1, do not use the FTP protocol for file transfers, as FTP is unsecure and deprecated. Instead, use SFTP (Secure File Transfer Protocol) or SCP (Secure Copy Protocol) for improved security, as they provide encrypted communication.

Periodic syslog warnings will be generated once every 30 days as long as FTP is configured.

Task ID

Task ID	Operations
ip-services	read, write

Examples

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

```
Router(config)# ftp client anonymous-password xxxx
```

ftp client passive

To configure the software to use only passive File Transfer Protocol (FTP) connections, use the **ftp client passive** command in XR Config 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 keywords or arguments.

Command Default

FTP data connections are active.

Command Modes

XR Config mode

Command History

Release	Modification
Release 25.4.1	The **ftp** keyword is deprecated.
Release 7.0.12	This command was introduced.

Usage Guidelines

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.

Starting with Cisco IOS XR Software Release 25.4.1, do not use the FTP protocol for file transfers, as FTP is unsecure and deprecated. Instead, use SFTP (Secure File Transfer Protocol) or SCP (Secure Copy Protocol) for improved security, as they provide encrypted communication.

Periodic syslog warnings will be generated once every 30 days as long as FTP is configured.

Task ID

Task ID	Operations
ip-services	read, write

Examples

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

```
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.
```

ftp client password

To specify the password for the File Transfer Protocol (FTP) connections, use the **ftp client password** command in XR Config mode. To disable this feature, use the **no** form of this command.

ftp client password {*clear-text-password* | **clear** *clear-text password* | **encrypted** *encrypted-text password*}
no ftp client password {*clear-text-password* | **clear** *clear-text password* | **encrypted** *encrypted-text password*}

Syntax Description

clear-text-password	Specifies an unencrypted (cleartext) user password
clear *clear-text password*	Specifies an unencrypted (cleartext) shared password.
encrypted *encrypted-text password*	Specifies an encrypted shared password.

Command Default

No default behavior or values

Command Modes

XR Config mode

Command History

Release	Modification
Release 25.4.1	The **ftp** keyword is deprecated.
Release 7.0.12	This command was introduced.

Usage Guidelines

Starting with Cisco IOS XR Software Release 25.4.1, do not use the FTP protocol for file transfers, as FTP is unsecure and deprecated. Instead, use SFTP (Secure File Transfer Protocol) or SCP (Secure Copy Protocol) for improved security, as they provide encrypted communication.

Periodic syslog warnings will be generated once every 30 days as long as FTP is configured.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to specify the password for the File Transfer Protocol (FTP) connections:

```
Router(config)# ftp client password lab
```

ftp client source-interface

To specify the source IP address for File Transfer Protocol (FTP) connections, use the **ftp client source-interface** command in XR Config 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 interface-path-id*
no ftp client source-interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

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

Command Modes

XR Config mode

Command History

Release	Modification
Release 25.4.1	The **ftp** keyword is deprecated.
Release 7.0.12	This command was introduced.

Usage Guidelines

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.

Starting with Cisco IOS XR Software Release 25.4.1, do not use the FTP protocol for file transfers, as FTP is unsecure and deprecated. Instead, use SFTP (Secure File Transfer Protocol) or SCP (Secure Copy Protocol) for improved security, as they provide encrypted communication.

Periodic syslog warnings will be generated once every 30 days as long as FTP is configured.

Task ID

Task ID	Operations
ip-services	read, write

Examples

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

```
Router(config)# ftp client source-interface HundredGigE0/1/2/1
```

ftp client username

To specify the username for File Transfer Protocol (FTP) connections, use the **ftp client username** command in XR Config mode. To disable this feature, use the **no** form of this command.

ftp client username *username*
no ftp client username *username*

Syntax Description

username	Name for FTP user.

Command Modes

XR Config mode

Command History

Release	Modification
Release 25.4.1	The **ftp** keyword is deprecated.
Release 7.0.12	This command was introduced.

Usage Guidelines

Starting with Cisco IOS XR Software Release 25.4.1, do not use the FTP protocol for file transfers, as FTP is unsecure and deprecated. Instead, use SFTP (Secure File Transfer Protocol) or SCP (Secure Copy Protocol) for improved security, as they provide encrypted communication.

Periodic syslog warnings will be generated once every 30 days as long as FTP is configured.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to specify the username for FTP connections:

```
Router(config)# ftp client username brownfox
```

http client connection

To configure the connection for http client, use the **http client connection** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client connection { **retry** *count* | **timeout** *seconds* }

Syntax Description

retry *count*	Specifies how many times HTTP Client resends a connection request. Range is from 1 to 5. The default value is 0.
timeout *seconds*	The time interval (in seconds) that HTTP client waits for a server connection to establish before giving up. Range is from 1 to 60 seconds. The default value is 10 seconds.

Command Default

The connection retry is not configured by default. The default connection timeout is set to 10 seconds.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use this command to set the connection timeout or connection retry count.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to configure the connection request retry to two times:

```
RP/0/RP0/CPU0:router(config)#http client connection retry 2
```

The following example shows how to configure the connection request timeout to 20 seconds:

```
RP/0/RP0/CPU0:router(config)#http client connection timeout 20
```

http client response

To configure the time interval (in seconds) for HTTP Client to wait for a response from the server before giving up, use the **http client response** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client response { **timeout** *seconds* }

Syntax Description

timeout *seconds*	The time interval (in seconds) that HTTP client waits for a response from the server before giving up. Range is from 1 to 300 seconds. The default value is 30 seconds.

Command Default

The response timeout is 30 seconds by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use this command to configure the response timeout.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to configure the response timeout to 40 seconds:

```
RP/0/RP0/CPU0:router(config)#http client response timeout 40
```

http client secure-verify-host

To enable verifying host in peer's certificate, use the **http client secure-verify-host** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client secure-verify-host

Syntax Description

secure-verify-host	Verifies the host in peer's certificate. This is enabled by default. To disable, use the command **http client secure-verify-host** *disable*

Command Default

Host verification is enabled by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **http client secure-verify-host** command to disable the host verification.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to disable host verification :

```
RP/0/RP0/CPU0:router(config)#http client secure-verify-host disable
```

http client secure-verify-peer

To enable verifying authenticity of the peer certificate, use the **http client secure-verify-peer** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client secure-verify-peer

Syntax Description

secure-verify-peer	Verifies authenticity of the peer certificate. This is enabled by default. To disable, use the command **http client secure-verify-peer** *disable*

Command Default

Peer verification is enabled by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **http client secure-verify-peer** command to disable the peer verification.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to disable peer verification :

```
RP/0/RP0/CPU0:router(config)#http client secure-verify-peer disable
```

http client source-interface

To specify the interface for source address for Hypertext Transfer Protocol (HTTP) connections, use the **http client source-interface** command in XR Config mode. To remove the **http client source-interface**command from the configuration file and restore the system to its default condition, use the **no** form of this command.

http client source-interface { **ipv4** | **ipv6** }

Syntax Description

ipv4 *ip-address*	Enter ipv4 address from interface.
ipv6 *ip-address*	Enter ipv6 address from interface.

Command Default

No default behavior or values.

Command History

Release	Modification
Release 7.10.1	This command was modified to configure both ipv4 and ipv6 source interfaces.
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **http client source-interface** command to configure ipv4 and ipv6 source interfaces. If both the source interfaces are configured, then the source interface is selected depending on the host DNS resolution.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to configure ipv4 source interface for HTTP connection:

```
RP/0/RP0/CPU0:router(config)#http client source-interface ipv4 gigabitEthernet 0/0/0/0
```

The following example shows how to configure ipv6 source interface for HTTP connection:

```
RP/0/RP0/CPU0:router(config)#http client source-interface ipv6 gigabitEthernet 0/0/0/0
```

http client ssl

To configure Secure Socket Layer (SSL) version to be used for HTTPS requests, use the **http client ssl** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client ssl *version*

Syntax Description

ssl *version*	Specify the SSL version to be used for HTTPS requests. Select one of the following versions: • **tls1.0** - Forces TLSv1.0 to be used for HTTPS requests. • **tls1.1** - Forces TLSv1.1 to be used for HTTPS requests. • **tls1.2** - Forces TLSv1.2 to be used for HTTPS requests. • **tls1.3** - Forces TLSv1.3 to be used for HTTPS requests. By default libcurl does not force the TLS version.

Command Default

By default, the SSL version is not configured.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.
Release 24.3.1	The support for SSL version TLS 1.3 was added.

Usage Guidelines

Use this command to configure the ssl version to be used in HTTPS requests.

Starting with Cisco IOS XR Software Release 25.4.1, a one-time syslog warning is generated if TLS 1.0 or TLS 1.1 is used, and a continuous warning once in a month occurs if the http client TLS version is configured as TLS 1.0 or 1.1. The default minimum syslog TLS version is now TLS 1.2 to enhance security.

Task ID

Task ID	Operations
config-servicess	read, write

The following example shows how to configure the SSL version to tls1.1:

```
RP/0/RP0/CPU0:router(config)#http client ssl tls1.1
```

http client tcp-window-scale

To configure the TCP window scale factor for high latency links, use the **http client tcp-window-scale** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client tcp-window-scale *scale*

Syntax Description

scale	Specify the TCP window scale for HTTP requests. Range is 1 to 14.

Command Default

By default, TCP window scale is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.3.6	This command was introduced.

Usage Guidelines

Use this command to configure the TCP window scale for HTTP requests.

Note Currently, this is enabled for copying of files using HTTP.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to set the TCP window scale to 10:

```
RP/0/RP0/CPU0:router(config)#http client tcp-window-scale 10
```

http client version

To configure the HTTP version to be used for HTTP requests, use the **http client version** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client version *version*

Syntax Description

version*version*	Specify the HTTP version to be used for HTTP requests. Select one of the following versions: • **1.0** - Forces HTTP1.0 to be used for all HTTP requests. • **1.1** - Forces HTTP1.1 to be used for all HTTP requests. • **default** - libcurl picks up HTTP version automatically.

Command Default

By default, libcurl does not force the HTTP version.

Note HTTP Client uses libcurl version 7.30

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use this command to configure the HTTP version to be used in HTTP requests.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to configure the HTTP version to 1.1:

```
Router(config)#http client version 1.1
```

http client vrf

To configure a new VRF to be used by the HTTP client, use the **http client vrf** command. To remove the specified vrf, use the **no** form of this command.

http client vrf *vrf-name*

Syntax Description

vrf-name	Specifies the name of the VRF to be used by the HTTP client.

Command Default

If not configured, the default VRF "default-vrf" will be used.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

A HTTP client can have only one VRF. If a specific VRF is not configured for the HTTP client, the default VRF is assumed.

Task ID

Task ID	Operations
config-services	read, write

The following example shows the HTTP client being configured to start with the specified VRF:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# http client vrf green
```

icmp ipv4 mpls extended-diagnostics

To configure extended-diagnostics mode, use the **icmp ipv4 mpls extended-diagnostics** command in XR Config mode. To remove the configuration, use the **no** form of this command.

icmp ipv4 mpls extended-diagnostics

Syntax Description

The command has no optional keywords or agruments.

Command Default

None

Command Modes

XR Config mode

Release	Modification
Release 25.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID	Operations
ipv4	read, write
network	read, write

Examples

This example shows how to enter the extended-diagnostics submode for icmp ipv4 mpls:

```
Router(config)# icmp ipv4 mpls
Router(config-icmp-ipv4)# extended-diagnostics
Router(config-icmp-ipv4-diag)# commit
```

icmp ipv4 vrf extended-diagnostics permitted-remote-address

To configure extended-diagnostics mode with permitted remote-address, use the **icmp ipv4 vrf** command in XR Config mode. To remove the configuration, use the **no** form of this command.

icmp ipv4 vrf *vrf-name* **extended-diagnostics permitted-remote-address** *permitted-ipv4-address-prefix*

Syntax Description

vrf-name	Specifies the name of the VRF.
permitted-ipv4-address-prefix	Specifies the address prefix to which ICMP replies with extended diagnostic information may be sent

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 25.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

This example shows how to configure the permitted-remote-address with extended-diagnostics submode for icmp ipv4 vrf:

```
Router#configure
Router(config)#icmp ipv4 vrf extended-diagnostics permitted-remote-address 192.0.2.0/24
Router(config-icmp-vrf-diag)#commit
```

icmp ipv6 mpls extended-diagnostics

To configure extended-diagnotics mode, use the **icmp ipv6 mpls extended-diagnostics** command in XR Config mode. To remove the extended-diagnostics mode, use the **no** form of this command.

icmp ipv6 mpls extended-diagnostics

Syntax Description

The command has no optional keywords or arguments.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 25.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

This example shows how to enter the extended-diagnostics submode for icmp ipv6 mpls:

```
Router(config)# icmp ipv6 mpls
Router(config-icmp-ipv6)# extended-diagnostics
Router(config-icmp-ipv6)# commit
```

icmp ipv6 vrf extended-diagnostics permitted-remote-address

To configure permitted-remote-address with extended-diagnostics mode, use the **icmp ipv6 vrf extended-diagnostics permitted-remote-address** command in XR Config mode . To remove the configuration, use the `no` form of this command.

icmp ipv6 vrf *vrf-name* **extended-diagnostics permitted-remote-address** *permitted-remote-ipv6-prefix*

Syntax Description

vrf-name	Specifies the name of the VRF.
permitted-ipv6-address-prefix	Specifies the address prefix to which ICMP replies with extended diagnostic information may be sent

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 25.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

This example shows how to configure the permited-remote-address with extended-diagnostics submode for icmp ipv6 vrf:

```
Router# configure
Router(config)# icmp ipv6 vrf extended-diagnostics permitted-remote-address 2001:db8::/32
Router(config-icmp-vrf-diag)# commit
```

logging source-interface vrf

To configure the logging source interface in order to identify the syslog traffic that originates in a VRF from a particular router, as coming from a single device, use the **logging source-interface vrf** command in XR Config mode. To remove the source-interface logging configuration for the given VRF, use the **no** form of this command.

logging source-interface *interface* **vrf** *vrf-name*
no logging source-interface *interface* **vrf** *vrf-name*

Syntax Description

interface	Interface number of the source
vrf-name	Name that identifies the VRF

Command Default

If *vrf-name* is not specified, the source interface is configured for the default VRF.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Normally, a syslog message contains the IPv4 or IPv6 address of the interface used to exit the router. The **logging source-interface** command configures the syslog packets to contain the IPv4 or IPv6 address of a particular interface for a VRF, regardless of which interface the packet uses to exit the router.

Task ID

Task ID	Operation
logging	read, write

Example

This example shows how to configure interface loopback 0 to be the logging source interface for VRF vrf1.

```
Router#logging source-interface loopback 0 vrf vrf1
Router#logging source-interface loopback 1 vrf default
```

This sample output shows a logging source interface that is correctly configured for the VRF.

```
Router#show running-config logging
Wed Mar 4 07:37:48.974 UTC
logging console disable
logging source-interface Loopback0 vrf vrf1
```

ping bulk (network)

To check reachability and network connectivity to multiple hosts on IP networks, use the **ping bulk** command in XR EXEC mode.

ping bulk ipv4 [**input cli** [**batch** | **inline**]]
[**vrf** *vrf-name*] [**ip-address** | **domain-name**]

Syntax Description

ipv4	Specifies IPv4 address prefixes.
input	Specifies input mode.
cli	Specifies input via CLI.
batch	Pings after all destinations are input.
inline	Pings after each destination is input.
vrf *vrf-name ip-address domain-name*	(Optional) Specifies a particular VRF. IP address of the system to ping. (Optional) Domain name of the system to ping. **Note** You must hit the Enter button and then specify one destination address per line.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

You must hit the Enter button and then specify one destination address per line.

Maximum number of destinations you can specify in the cli or batch mode is 2000.

Task ID

Task ID	Operation
basic-services	read, write, execute

Example

The following example shows how to ping many hosts by the input via CLI method:

```
Router# ping bulk ipv4 input cli batch
```

```
Please enter input via CLI with one destination per line and when done Ctrl-D/(exit)
to initiate pings:
1: vrf myvrf1 10.2.1.16
2:
Starting pings...
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.1.16, vrf is myvrf1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/9 ms



Router# ping bulk ipv4 input cli

Please enter input via CLI with one destination per line:
vrf myvrf1 1.1.1.1
vrf myvrf2 2.2.2.2
vrf myvrf1 myvrf1.cisco.com
vrf myvrf2 myvrf2.cisco.com

Starting pings...
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 1.1.1.1, vrf is myvrf1:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/1 ms
Sending 2, 100-byte ICMP Echos to 2.2.2.2, vrf is myvrf2:
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
Sending 1, 100-byte ICMP Echos to 1.1.1.1, vrf is myvrf1:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/4/1 ms
Sending 2, 100-byte ICMP Echos to 2.2.2.2, vrf is myvrf2:
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/3/1 ms
```

ping (network)

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

ping [**ipv4** | **ipv6**] [*host-nameip-address*] [**count** *number*] [**size** *number*] [**source** {*ip-addressinterface-name* | **type** *number*}] [**timeout** *seconds*] [**pattern** *number*] [**type** *number*] [**priority** *number*][**verbose**] [**donnotfrag**] [**validate**] [**sweep**]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
A.B.C.D	Target end address of the pseudowire.
host-name	(Optional) Hostname of the system to ping.
ip-address	(Optional) IP address of the system to ping.
count *number*	(Optional) Sets the repeat count. Range is 0 to 2147483647.
size *number*	(Optional) Sets the datagram size. Range is 36 to 18024
source	(Optional) Identifies the source address or source interface.
type *number*	(Optional) Sets the type of service. Range is 0 to 255. Available when the **ipv4** keyword is specified.
timeout *seconds*	(Optional) Sets the timeout in seconds. Range is 0 to 3600.
priority *number*	(Optional) Sets the packet priority. Range is 0 to 15. Available when the **ipv6** keyword is specified.
pattern *number*	(Optional) Sets the data pattern. Range is 0 to 65535.
verbose	(Optional) Sets verbose output.
donnotfrag	(Optional) Sets the Don't Fragment (DF) bit in the IP header.
validate	(Optional) Validates the return packet.
sweep	(Optional) Sets the sweep ping.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The default value for the **ping** command refers only to the target IP address. No default value is available for the target IP address.

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 hostname or an 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 hostname, it returns an "%Unrecognized host or address, or protocol not running" error message.

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

This table 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 protocol data unit (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 does not fragment the packet and returns an Internet Control Message Protocol (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 to forward it to the next hop.
Q	A source quench packet was received.

Task ID

Task ID	Operations
basic-services	read, write, execute

Examples

Although the precise dialog varies somewhat between IPv4 and IPv6, all are similar to the ping session, using default values shown in the following output:

```
Router# ping

Protocol [ipv4]:
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 hostname or an address on the same line as the **ping** command, the command performs the default actions appropriate for the protocol type of that hostname or address, as shown in the following output:

```
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
```

probe

To query the status of a probed interface IP networks, use the **probe** command in XR EXEC mode.

probe *proxy-address-or-hostname* [**by-name** *probed-interface-name*] [**by-remote-address** *probed-interface-address*] [**count** *number*] [**hop-count** *number*] [**source** { *ip-address* *interface-name* }] [**timeout** *seconds*] [**vrf** *vrf-table*]

Syntax Description

proxy-address-or-hostname	Specifies the name of the proxy-address or hostname to be probed.
by-name *probed-interface-name*	(Optional) Specifies the interface name to query at the destination
by-remote-address *probed-interface-address*	(Optional) Specifies the remote address to query at the destination
count *number*	(Optional) Specifies the repeat count in the range of 1-255.
source	(Optional) Identifies the source address or source interface.
hop-count *number*	(Optional) Sets the TTL value of the probe. Range is 0 to 255.
timeout *seconds*	(Optional) Sets the timeout in seconds. Range is 0 to 3600.
vrf	(Optional) Specifies the vrf table for route lookup.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 25.4.1	This command was introduced.

Usage Guidelines

When using the probe command, you may specify the target as either a proxy address or a hostname. If a hostname is provided, the application will resolve it to an IPv4 or IPv6 address—prioritizing IPv6 if available—and emit the probe accordingly, as per RFC 8335. The source address can be specified directly or as a network interface; if an interface is given, any valid address from that interface may be used. If no source is specified, default logic is applied. Specifying a source by name automatically sets the local flag, while specifying by remote address clears it. The Hop Count parameter is used to set the IPv4 TTL or IPv6 Hop Count for the probe packet.

Task ID

Task ID	Operations
basic-services	read, write, execute

Examples

This is an example of using probe command between interface IP networks:

```
Router# probe 192.168.1.10 source Loopback0 by-name BVI1
PROBE 192.168.1.9 -> 192.168.1.10
```

```
8 bytes from 192.168.1.10: icmp_seq=0 ttl=64 time=1.202 ms. Interface=BVI1
8 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=1.089 ms. Interface=BVI1
8 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=1.115 ms. Interface=BVI1
```

scp

To securely transfer a file from a local directory to a remote directory or from a remote directory to a local directory, use the **scp** command in XR EXEC mode.

scp {*local-directory username@location/directory*} */ filename* {*username@location/directory local-directory* } */ filename*

Syntax Description

local-directory	Specifies the local directory on the device.
username@location/directory	Specifies the remote directory where *location* is the IP address of the remote device.
filename	Specifies the file name to be transferred.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Secure Copy Protocol (SCP) is a file transfer protocol which provides a secure and authenticated method for transferring files. SCP relies on SSHv2 to transfer files from a remote location to a local location or from local location to a remote location.

Use the **scp** command to copy a file from the local device to a destination device or from a destination device to the local device.

Using SCP, you can only transfer individual files. You cannot transfer a file from a remote device to another remote device.

SSH server process must be running on the remote device.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to copy a file using the **scp** command from a local directory to a remote directory:

```
Router# scp /usr/file1.txt root@209.165.200.1:/root/file3.txt

Connecting to 209.165.200.1...
Password:
  Transferred 553065 Bytes
  553065 bytes copied in 0 sec (7576232)bytes/sec
```

The following example shows how to copy a file using the **scp** command from a remote directory to a local directory:

```
Router# scp root@209.165.200.1:/root/file4.txt /usr/file.txt

Connecting to 209.165.200.1...
Password:
  Transferred 553065 Bytes
  553065 bytes copied in 0 sec (7576232)bytes/sec
```

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 XR Exec mode.

show cinetd services

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.5.4	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read

Examples

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

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

Vrf Name          Family Service Proto Port ACL max_cnt curr_cnt wait Program Client Option

context-management v4    tftp   udp   69      unlimited       0    wait ttfpd sysdb  disk0:
default            v4    telnet   tcp   23       100       2    nowait telnetd sysdb  disk0
```

This table describes the significant fields shown in the display.

Table 2: show cinetd services Command Field Descriptions

Field	Description
Family	Version of the network layer (IPv4 or IPv6).
Service	Network service (for example, FTP, Telnet, and so on).
Proto	Transport protocol used by the service (tcp or udp).
Port	Port number used by the service.
ACL	Access list used to limit the service from some hosts.
max_cnt	Maximum number of concurrent servers allowed for a service.

Field	Description
curr_cnt	Current number of concurrent servers for a service.
wait	Status of whether Cinetd has to wait for a service to finish before serving the next request.
Program	Name of the program for a service.
Option	Service-specific options.

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 hostnames and addresses, use the **show hosts** command in XR EXEC mode.

show hosts [*host-name*]

Syntax Description

host-name	(Optional) Name of the host about which to display information. If omitted, all entries in the local cache are displayed.

Command Default

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

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read

Examples

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

```
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
```

This table describes the significant fields shown in the display.

Table 3: show hosts Command Field Descriptions

Field	Description
Default domain	Default domain used to complete the unqualified hostnames.
Name/address lookup	Lookup is disabled or uses domain services.
Name servers	List of configured name servers.
Host	Hostname.

Field	Description
Flags	Indicates the status of an entry. • temp—Temporary entry entered by a name server; the software removes the entry after 72 hours of inactivity. • perm—Permanent entry entered by a configuration command; does not time out. • OK—Entry is believed to be valid. • ??—Entry is considered suspect and subject to revalidation. • EX—Entry has expired.
Age(hr)	Number of hours since the software most recently referred to the cache entry.
Type	Type of address (IPv4 or IPv6).
Address(es)	Address of the host. One host may have up to eight addresses.

telnet

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

telnet [**vrf** {*vrf-name* | **default**}] {*ip-address* | *host-name*} [*options*]

Syntax Description

vrf	(Optional) Specifies a VPN routing and forwarding (VRF) instance
vrf-name	VRF name of the system to ping.
default	Specifies the default VRF instance.
ip-address	IP address of a specific host on a network. • IPv4 address format—Must be entered in the (*x.x.x.x*) format. • IPv6 address format— Must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host-name	Name of a specific host on a network.
options	(Optional) Telnet connection options. See **Telnet Connection Options** for a list of supported options.

Command Default

Telnet client is in Telnet connection options nostream mode.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 25.4.1	This command is deprecated.
Release 7.0.12	This command was introduced.

Usage Guidelines

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.

This table lists the supported Telnet connection options.

Table 4: Telnet Connection Options

Option	Description
/stream	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 UNIX-to-UNIX copy program (UUCP) and other non-Telnet protocols.
/nostream	Turns off stream processing.
port number	Port number. Range is 0 to 65535.
/source-interface	Specifies 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 hostname, 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. **Special Telnet Escape Sequences** lists the special Telnet escape sequences.

Table 5: Special Telnet Escape Sequences

Escape Sequence[1]	Purpose
Ctrl-^ c	Interrupt Process (IP).
Ctrl-^ o	Terminates 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-^?

Starting with Cisco IOS XR Software Release 25.4.1, do not use the telnet protocol for logging in, as telnet is unsecure and deprecated. Instead, use SSHv2 (Secure Shell Version 2) for improved security, as it provides encrypted communication.

Periodic syslog warnings will be generated once every 30 days as long as telnet is configured.

Task ID

Task ID	Operations
basic-services	read, write, execute

Examples

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

```
Router# telnet host1
```

telnet client source-interface

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

telnet {**ipv4** | **ipv6**} **client source-interface** *type interface-path-id*
no telnet client source-interface *type interface-path-id*

Syntax Description

ipv4	Specifies IPv4 address prefixes.
ipv6	Specifies IPv6 address prefixes.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

The IP address of the best route to the destination is used as the source IP address.

Command Modes

XR Config mode

Command History

Release	Modification
Release 25.4.1	This command is deprecated.
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **telnet client source-interface** command to set the IP address of an interface as the source for all Telnet connections.

Starting with Cisco IOS XR Software Release 25.4.1, do not use the telnet protocol for logging in, as telnet is unsecure and deprecated. Instead, use SSHv2 (Secure Shell Version 2) for improved security, as it provides encrypted communication.

Periodic syslog warnings will be generated once every 30 days as long as telnet is configured.

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

Examples

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

```
Router(config)# telnet ipv4 client source-interface hundredgige1/0/2/1
```

telnet dscp

To define the differentiated services code point (DSCP) value and IPv4 precedence to specifically set the quality-of-service (QoS) marking for Telnet traffic on a networking device, use the **telnet dscp** command in XR Config mode. To disable DSCP, use the **no** form of this command.

telnet [**vrf** {*vrf-name* | **default**}] **ipv4 dscp** *dscp-value*
no telnet [**vrf** {*vrf-name* | **default**}] **ipv4 dscp** *dscp-value*

Syntax Description

vrf	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF name of the system to ping.
default	(Optional) Specifies the default VRF instance.
ipv4	Specifies IPv4 address prefixes.
dscp-value	Value for DSCP. The range is from 0 to 63. The default value is 0.

Command Default

If DSCP is disabled or not configured, the following default values are listed:

- The default value for the server 16.
- The default value for the client is 0.

Command Modes

XR Config mode

Command History

Release	Modification
Release 25.4.1	This command is deprecated.
Release 7.0.12	This command was introduced.

Usage Guidelines

IPv4 is the supported protocol for defining a DSCP value for locally originated Telnet traffic.

DSCP can impact both server and client behavior of the specific VRF.

Starting with Cisco IOS XR Software Release 25.4.1, do not use the telnet protocol for logging in, as telnet is unsecure and deprecated. Instead, use SSHv2 (Secure Shell Version 2) for improved security, as it provides encrypted communication.

Periodic syslog warnings will be generated once every 30 days as long as telnet is configured.

Task ID

Task ID	Operations
ipv4	read, write

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to define the DSCP value and IPv4 precedence:

```
Router(config)# telnet vrf default ipv4 dscp 40
Router(config)# telnet vrf default ipv4 dscp 10
```

telnet server

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

telnet [**vrf** {*vrf-name* | **default**}] {**ipv4** | **ipv6**} **server max-servers** {**no-limit***limit*} [**access-list** *list-name*]
no telnet [**vrf** {*vrf-name* | **default**}] {**ipv4** | **ipv6**} **server max-servers** {**no-limit***limit*} [**access-list** *list-name*]

Syntax Description

vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF name of the system to ping.
default	(Optional) Specifies the default VRF instance.
ipv4	Specifies IPv4 address prefixes.
ipv6	Specifies IPv6 address prefixes.
max-servers	Sets the number of allowable Telnet servers.
no-limit	Specifies that there is no maximum number of allowable Telnet servers.
limit	Specifies the maximum number of allowable Telnet servers. Range is 1 to 200.
access-list	(Optional) Specifies an access list.
list-name	(Optional) Access list name.

Command Default

Telnet services are disabled.

Command History

Release	Modification
Release 25.4.1	This command is deprecated.
Release 7.0.12	This command was introduced.

Usage Guidelines

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 are accepted, and the Cisco Internet services daemon (Cinetd) stops listening on the Telnet port.

Enable Telnet services by setting the **max-servers** keyword to a value of one or greater. This allows 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 disables the Telnet connection and restores the system to its default condition.

Starting with Cisco IOS XR Software Release 25.4.1, do not use the telnet protocol for logging in, as telnet is unsecure and deprecated. Instead, use SSHv2 (Secure Shell Version 2) for improved security, as it provides encrypted communication.

Periodic syslog warnings will be generated once every 30 days as long as telnet is configured.

Note Before establishing communications with the router through a Telnet session, configure the telnet server and vty-pool functions (see *System Management Command Reference for Cisco 8000 Series Routers*, *System Management Configuration Guide for Cisco 8000 Series Routers*, and *IP Addresses and Services Configuration Guide for Cisco 8000 Series Routers*.

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

Examples

The following example shows how to enable Telnet services for one server:

```
Router(config)# telnet ipv4 server max-servers 1
```

telnet transparent

To send a Carriage Return (CR) as a CR-NULL rather than a Carriage Return-Line Feed (CR-LF) for virtual terminal sessions, use the **telnet transparent** command in line template submode. 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 keywords or arguments.

Command Default

No default behavior or values

Command Modes

Line console

Command History

Release	Modification
Release 25.4.1	This command is deprecated.
Release 7.0.12	This command was introduced.

Usage Guidelines

The **telnet transparent** command is useful for coping with different interpretations of end-of-line handling in the Telnet protocol specification.

Starting with Cisco IOS XR Software Release 25.4.1, do not use the telnet protocol for logging in, as telnet is unsecure and deprecated. Instead, use SSHv2 (Secure Shell Version 2) for improved security, as it provides encrypted communication.

Periodic syslog warnings will be generated once every 30 days as long as telnet is configured.

Task ID

Task ID	Operations
tty-access	read, write

Examples

The following example shows how to configure the vty line to operate in Telnet transparent mode so that when the carriage return key is pressed the system sends the signal as a CR-NULL key combination rather than a CR-LF key combination:

```
Router(config)# line console
Router(config-line)# telnet transparent
```

tftp server

To enable or disable the TFTP server or a feature running on the TFTP server, use the **tftp server** command in XR Config mode.

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

Syntax Description

ipv4	Specifies IPv4 address prefixes.
ipv6	Specifies IPv6 address prefixes.
homedir *tftp-home-directory*	Specifies the home directory.
max-servers *number*	(Optional) Sets the maximum number of concurrent TFTP servers. The range is from 1 to 2147483647.
max-servers no-limit	(Optional) Sets no limit to process a number of allowable TFTP server.
access-list *name*	(Optional) Specifies the name of the access list associated with the TFTP server.

Command Default

The TFTP server is disabled by default. When not specified, the default value for the **max-servers** keyword is unlimited.

Command Modes

XR Config mode

Command History

Release	Modification
Release 25.4.1	The **tftp** keyword is deprecated.
Release 7.5.4	This command was introduced.

Usage Guidelines

Using the **no** form of the **tftp server** 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.

Starting with Cisco IOS XR Software Release 25.4.1, do not use the TFTP for file transfers, as TFTP is unsecure and deprecated. Instead, use SFTP (Secure File Transfer Protocol) or SCP (Secure Copy Protocol) for improved security, as they provide encrypted communication.

Periodic syslog warnings will be generated once every 30 days as long as TFTP is configured.

Task ID

Task ID	Operations
ipv4	read, write

Task ID	Operations
ip-services	read, write

Examples

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

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

tftp client source-interface

To specify the source IP address for a TFTP connection, use the **tftp client source-interface** command in XR Config 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 interface-path-id*
no tftp client source-interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

The IP address of the best route to the destination is used as the source IP address.

Command Modes

XR Config mode

Command History

Release	Modification
Release 25.4.1	The **tftp** keyword is deprecated.
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **tftp client source-interface** command to set the IP address of an interface as the source for all TFTP connections.

Starting with Cisco IOS XR Software Release 25.4.1, do not use the TFTP for file transfers, as TFTP is insecure and deprecated. Instead, use SFTP (Secure File Transfer Protocol) or SCP (Secure Copy Protocol) for improved security, as they provide encrypted communication.

Periodic syslog warnings will be generated once every 30 days as long as TFTP is configured.

Task ID

Task ID	Operations
ip-services	read, write

Examples

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

```
Router(config)# tftp client source-interface hundredgige1/0/2/1
```

traceroute

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

traceroute [**ipv4** | **ipv6**] [*host-name ip-address*] [{ **source** *ip-address-name interface-name* }] [**numeric**] [**timeout** *seconds*] [**probe** *count*] [**minttl** *seconds*] [**maxttl** *seconds*] [**port** *number*] [**priority** *number*] [**verbose**] [**extended**]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.
host-name	(Optional) Hostname of system to use as the destination of the trace attempt.
ip-address	(Optional) Address of system to use as the destination of the trace attempt.
source	(Optional) Source address.
ip-address-name	(Optional) IP address A.B.C.D or hostname.
numeric	(Optional) Numeric display only.
timeout *seconds*	(Optional) Timeout value. Range is 0 to 3600.
probe *count*	(Optional) Probe count. Range is 0 to 65535.
minttl *seconds*	(Optional) Minimum time to live. Range is 0 to 255.
maxttl *seconds*	(Optional) Maximum time to live. Range is 0 to 255.
port *number*	(Optional) Port number. Range is 0 to 65535.
priority *number*	(Optional) Packet priority. Range is 0 to 15. Available when the **ipv6** keyword is specified.
verbose	(Optional) Verbose output.
extended	(Optional) Displays any of the additional extended diagnostic information if available.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 25.4.1	This command was modified to include the **extended** keyword.
Release 7.0.12	This command was introduced.

Usage Guidelines

The default value for the **traceroute** command refers only to the destination. No default value is available for the destination address.

The **traceroute** 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** 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** command sends several probes at each TTL level and displays the round-trip time for each.

The **traceroute** 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, the **traceroute** command prints an asterisk (*).

The **traceroute** 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 interactive **traceroute** test, enter the command without a *host-name* or *ip- address* argument. You are stepped through a dialog to select the desired parameter values for the **traceroute** test.

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

Not all destinations 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, the **traceroute** command times out on responses 6 through 11.

Task ID

Task ID	Operations
basic-services	read, write, execute

Examples

The following output shows a sample **traceroute** session when a destination hostname has been specified:

```
Router# traceroute 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 interactive **traceroute** session when a destination hostname is not specified:

```
traceroute# traceroute

Protocol [ipv4]:
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-jpxlnock-vpn.cisco.com (10.25.0.1) 30 msec  4 msec  4 msec
 2  15lab-vlan725-gx1.cisco.com (173.19.72.2) 7 msec  5 msec  5 msec
 3  stc15-00lab-gw1.cisco.com (173.24.114.33) 5 msec  6 msec  6 msec
 4  stc5-lab4-gw1.cisco.com (173.24.114.89) 5 msec  5 msec  5 msec
 5  stc5-sbb4-gw1.cisco.com (172.71.241.162) 5 msec  6 msec  6 msec
 6  stc5-dc5-gw1.cisco.com (172.71.241.10) 6 msec  6 msec  5 msec
 7  stc5-dc1-gw1.cisco.com (172.71.243.2) 7 msec  8 msec  8 msec
 8  ena-view3.cisco.com (172.71.164.199) 6 msec  *  8 msec
```

This table describes the characters that can appear in traceroute output.

Table 6: traceroute Text Characters

Character	Description
xx msec	For each node, the round-trip time in milliseconds for the specified number of probes.
*	Probe time 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.