Implementing Host Services and Applications

Cisco IOS XR software Host Services and Applications features on the router are used primarily for checking network connectivity and the route a packet follows to reach a destination, mapping a hostname to an IP address or an IP address to a hostname, and transferring files between routers and UNIX workstations.

Note For detailed conceptual information about Cisco IOS XR software Host Services and Applications and complete descriptions of the commands listed in this module, see the

Host Services and Applications Commands module in *IP Addresses and Services Command Reference for Cisco NCS 6000 Series Routers*

.

Feature History for Implementing Host Services and Applications

Release	Modification
Release 5.0.0	This feature was introduced.

- Prerequisites for Implementing Host Services and Applications , on page 1
- Information About Implementing Host Services and Applications , on page 2
- How to Implement Host Services and Applications , on page 4
- Configuration Examples for Implementing Host Services and Applications , on page 11
- Additional References, on page 13

Prerequisites for Implementing Host Services and Applications

The following prerequisites are required to implement Cisco IOS XR software Host Services and applications

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Information About Implementing Host Services and Applications

To implement Cisco IOS XR software Host Services and applications features discussed in this document, you should understand the following concepts:

Key Features Supported in the Cisco IOS XR software Host Services and Applications Implementation

The following features are supported for host services and applications on Cisco IOS XR software:

- Ping and traceroute—The **ping** and **traceroute** commands are convenient, frequently used tools for checking network connectivity and troubleshooting network problems. The **ping** command determines whether a specific IP address is online by sending out a packet and waiting for a response. The **traceroute** command provides the path from the source to the remote destination being contacted.
- Domain services—The domain services act as a Berkeley Software Distribution (BSD) domain resolver. When an application requires the IP address of a hostname or the hostname of an IP address, the domain services attempt to find the address or hostname by checking the local cache. If there is no address entry in the cache, a Domain Name System (DNS) query is sent to the name server. After the address or hostname is retrieved from the name server, the address or hostname is given to the application.
- File transfer services (FTP, TFTP)—FTP, TFTP clients are implemented as resource managers. The resource managers are mainly used for transferring files to and from a remote host and to place core files on a remote host. See the *File System Commands* module of the *System Management Configuration Guide for the Cisco NCS 6000 Series Router* for information on file transfer protocols.
- Cisco Inetd—Cisco Internet services daemon (Cinetd) is similar to UNIX inetd, in that it listens on a well-known port on behalf of the server program. When a service request is received on the port, Cinetd notifies the server program associated with the service request. By default, Cinetd is not configured to listen for any services. Cinetd is enabled by default. See the *Interface and Hardware Component Command Reference for the Cisco NCS 6000 Series Routers* for information on supported Cinetd commands.

Network Connectivity Tools

Network connectivity tools enable you to check device connectivity by running traceroutes and pinging devices on the network.

Ping

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

The **ping** command first sends an echo request packet to an address, and then it waits for a reply. The ping is successful only if the echo request gets to the destination, and the destination is able to get an echo reply (hostname is alive) back to the source of the ping within a predefined time interval.

Traceroute

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

The **traceroute** command records the source of each ICMP "time-exceeded" message to provide a trace of the path that the packet took to reach the destination. You can use the IP **traceroute** command to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

The **traceroute** command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. The **traceroute** command sends a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an ICMP time-exceeded message to the sender. The traceroute facility determines the address of the first hop by examining the source address field of the ICMP time-exceeded message.

To identify the next hop, the **traceroute** command sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-exceeded message to the source. This process continues until the TTL increments to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To determine when a datagram reaches its destination, the **traceroute** command sets the UDP destination port in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram with an unrecognized port number, it sends an ICMP port unreachable error to the source. This message indicates to the traceroute facility that it has reached the destination.

Domain Services

Cisco IOS XR software domain services acts as a Berkeley Standard Distribution (BSD) domain resolver. The domain services maintains a local cache of hostname-to-address mappings for use by applications, such as Telnet, and commands, such as **ping** and **traceroute** . The local cache speeds the conversion of hostnames to addresses. Two types of entries exist in the local cache: static and dynamic. Entries configured using the **domain ipv4 host** or **domain ipv6 host** command are added as static entries, while entries received from the name server are added as dynamic entries.

The name server is used by the World Wide Web (WWW) for translating names of network nodes into addresses. The name server maintains a distributed database that maps hostnames to IP addresses through the DNS protocol from a DNS server. One or more name servers can be specified using the **domain name-server** command.

When an application needs the IP address of a host or the hostname of an IP address, a remote-procedure call (RPC) is made to the domain services. The domain service looks up the IP address or hostname in the cache, and if the entry is not found, the domain service sends a DNS query to the name server.

You can specify a default domain name that Cisco IOS XR software uses to complete domain name requests. You can also specify either a single domain or a list of domain names. Any IP hostname that does not contain a domain name has the domain name you specify appended to it before being added to the host table. To specify a domain name or names, use either the **domain name** or **domain list** command.

TFTP Server

It is too costly and inefficient to have a machine that acts only as a server on every network segment. However, when you do not have a server on every segment, your network operations can incur substantial time delays across network segments. You can configure a router to serve as a TFTP server to reduce costs and time delays in your network while allowing you to use your router for its regular functions.

Typically, a router that is configured as a TFTP server provides other routers with system image or router configuration files from its flash memory. You can also configure the router to respond to other types of services requests.

File Transfer Services

File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP) are implemented as file systems or resource managers. For example, pathnames beginning with tftp:// are handled by the TFTP resource manager.

The file system interface uses URLs to specify the location of a file. URLs commonly specify files or locations on the WWW. However, on Cisco routers, URLs also specify the location of files on the router or remote file servers.

When a router crashes, it can be useful to obtain a copy of the entire memory contents of the router (called a core dump) for your technical support representative to use to identify the cause of the crash. FTP, TFTP can be used to save the core dump to a remote server. See the *System Management Configuration Guide for Cisco NCS 6000 Series Routers* for information on executing a core dump.

FTP

File Transfer Protocol (FTP) is part of the TCP/IP protocol stack, which is used for transferring files between network nodes. FTP is defined in RFC 959.

TFTP

Trivial File Transfer Protocol (TFTP) is a simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).

Cisco inetd

Cisco Internet services process daemon (Cinetd) is a multithreaded server process that is started by the system manager after the system has booted. Cinetd listens for Internet services such as Telnet service, TFTP service, and so on. Whether Cinetd listens for a specific service depends on the router configuration. For example, when the **tftp server** command is entered, Cinetd starts listening for the TFTP service. When a request arrives, Cinetd runs the server program associated with the service.

Telnet

Enabling Telnet allows inbound Telnet connections into a networking device.

How to Implement Host Services and Applications

This section contains the following procedures:

Checking Network Connectivity

As an aid to diagnosing basic network connectivity, many network protocols support an echo protocol. The protocol involves sending a special datagram to the destination host, then waiting for a reply datagram from that host. Results from this echo protocol can help in evaluating the path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

SUMMARY STEPS

1. **ping** [**ipv4** | **ipv6**] [*host-name* | *ip-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ping** [**ipv4** | **ipv6**] [*host-name* | *ip-address*] **Example:** `RP/0/RP0/CPU0:router# ping`	Starts the ping tool that is used for testing connectivity. **Note** If you do not enter a hostname or an IP 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.

Checking Packet Routes

The **traceroute** command allows you to trace the routes that packets actually take when traveling to their destinations.

SUMMARY STEPS

1. **traceroute** [**ipv4** | **ipv6**] [*host-name* | *ip-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**traceroute** [**ipv4** | **ipv6**] [*host-name* | *ip-address*] **Example:** `RP/0/RP0/CPU0:router# traceroute`	Traces packet routes through the network. **Note** If you do not enter a hostname or an IP address on the same line as the **traceroute** 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.

Configuring Domain Services

This task allows you to configure domain services.

Before you begin

DNS-based hostname-to-address translation is enabled by default. If hostname-to-address translation has been disabled using the **domain lookup disable** command, re-enable the translation using the **no domain lookup disable** command. See the *IP Addresses and Services Command Reference for Cisco NCS 6000 Series Routers* for more information on the **domain lookup disable** command.

SUMMARY STEPS

1. **configure**
2. Do one of the following:
    - **domain name** *domain-name*
    - or
    - **domain list** *domain-name*
3. **domain name-server** *server-address*
4. **domain** {**ipv4** | **ipv6**} **host** *host-name* {*ipv4address* | *ipv6address*}
5. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	

Step 2	Do one of the following:
	• **domain name** *domain-name*
	• or
	• **domain list** *domain-name*
	Example:
	`RP/0/RP0/CPU0:router(config)# domain name cisco.com`
	`or`
	`RP/0/RP0/CPU0:router(config)# domain list domain1.com`
		Defines a default domain name used to complete unqualified hostnames.

Step 3	**domain name-server** *server-address* **Example:** `RP/0/RP0/CPU0:router(config)# domain name-server 192.168.1.111`	Specifies the address of a name server to use for name and address resolution (hosts that supply name information). **Note** You can enter up to six addresses, but only one for each command.
Step 4	**domain** {**ipv4** | **ipv6**} **host** *host-name* {*ipv4address* | *ipv6address*} **Example:**	(Optional) Defines a static hostname-to-address mapping in the host cache using . **Note** You can bind up to eight additional associated addresses to a hostname.

	Command or Action	Purpose
	`RP/0/RP0/CPU0:router(config)# domain ipv4 host1 192.168.7.18`	
Step 5	**commit**	

Configuring a Router as a TFTP Server

This task allows you to configure the router as a TFTP server so other devices acting as TFTP clients are able to read and write files from and to the router under a specific directory, such as slot0:, /tmp, and so on (TFTP home directory).

Note For security reasons, the TFTP server requires that a file must already exist for a write request to succeed.

Before you begin

The server and client router must be able to reach each other before the TFTP function can be implemented. Verify this connection by testing the connection between the server and client router (in either direction) using the **ping** command.

SUMMARY STEPS

1. **configure**
2.
3. **commit**
4. show cinetd services

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**Example:** `RP/0/RP0/CPU0:router(config)# tftp ipv4 server homedir /tmp access-list listA homedir disk0`	Specifies: • IPv4 or IPv6 address prefixes (required) • Home directory (required) • Maximum number of concurrent TFTP servers (required) • Name of the associated access list (optional)
Step 3	**commit**	
Step 4	show cinetd services **Example:** `RP/0/RP0/CPU0:router# show cinetd services`	Displays the network service for each process. The service column shows TFTP if the TFTP server is configured.

Configuring a Router to Use FTP Connections

This task allows you to configure the router to use FTP connections for transferring files between systems on the network. With the implementation of FTP, you can set the following FTP characteristics:

- Passive-mode FTP
- Password
- IP address

SUMMARY STEPS

1. **configure**
2. **ftp client passive**
3. **ftp client anonymous-password** *password*
4. **ftp client source-interface** *type interface-path-id*
5. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ftp client passive** **Example:** `RP/0/RP0/CPU0:router(config)# ftp client passive`	Allows the software to use only passive FTP connections.
Step 3	**ftp client anonymous-password** *password* **Example:** `RP/0/RP0/CPU0:router(config)# ftp client anonymous-password xxxx`	Specifies the password for anonymous users.
Step 4	**ftp client source-interface** *type interface-path-id* **Example:** `RP/0/RP0/CPU0:router(config)# ftp client source-interface HundredGigE 0/1/2/1`	Specifies the source IP address for FTP connections.
Step 5	**commit**	

Troubleshooting Tips

When using FTP to copy any file from a source to a destination, use the following path format:

```
copy ftp
://
username:password
@
```

```
{
hostname
 |
ipaddress
}/
directory-path
/
pie-name target-device
```

When using an IPv6 FTP server, use the following path format:

```
copy ftp
:
//username
:
password
@
[ipv6-address]/
directory-path
/
pie-name
```

If unsafe or reserved characters appear in the username, password, hostname, and so on, they have to be encoded (RFC 1738).

The following characters are unsafe:

```
“<“, “>”, “#”, “%” “{“, “}”, “|”, “□”, “~”, “[“, “]”, and “‘”
```

The following characters are reserved:

```
“:”, “/” “?”, “:”, “@”, and “&”
```

The *directory-path* is a relative path to the home directory of the user. The slash (/) has to be encoded as %2f to specify the absolute path. For example:

```
ftp://user:password@hostname/%2fTFTPboot/directory/pie-name
```

See the **copy** command in the *System Management Command Reference for Cisco NCS 6000 Series Routers* for detailed information on using FTP protocol with the **copy** command.

Configuring a Router to Use TFTP Connections

This task allows you to configure a router to use TFTP connections. You must specify the source IP address for a TFTP connection.

SUMMARY STEPS

1. **configure**
2. **tftp client source-interface** *type*

3. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**tftp client source-interface** *type* **Example:** `RP/0/RP0/CPU0:router(config)# tftp client source-interface HundredGigE 1/0/2/1`	Specifies the source IP address for TFTP connections.
Step 3	**commit**	

Troubleshooting Tips

When using TFTP to copy any file from a source to a destination, use the following path format:

```
copy tftp
://{
hostname
 |
ipaddress
}/
directory-path
/
pie-name target-device
```

When using an IPv6 TFTP server, use the following path format:

```
copy tftp
:
//
[ipv6-address]/
directory-path
/
pie-name
```

See the **copy** command in the *System Management Command Reference for Cisco NCS 6000 Series Routers* for detailed information on using TFTP protocol with the **copy** command.

Configuring Telnet Services

This task allows you to configure Telnet services.

SUMMARY STEPS

1. **configure**
2. **telnet** [**ipv4** | **ipv6** |] **server max-servers 1**
3. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**telnet** [**ipv4** | **ipv6** |] **server max-servers 1** **Example:** `RP/0/RP0/CPU0:router(config)# telnet ipv4 server max-servers 1`	Enables one inbound Telnet server on the router. **Note** This command affects only inbound Telnet connections to the router.
Step 3	**commit**	

Configuration Examples for Implementing Host Services and Applications

This section provides the following configuration examples:

Checking Network Connectivity: Example

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

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

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

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

In this example, the extended **ping** command verifies the IP connectivity between the two IP addresses 10.0.0.2 and 10.0.0.1.

```
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
```

The **traceroute** command is used to discover the paths packets take to a remote destination and where routing breaks down. The **traceroute** command provides the path between the two IP addresses and does not indicate any problems along the path.

```
traceroute

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-jpollock-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
```

Configuring Domain Services: Example

The following example shows how to configure domain services on a router.

Defining the Domain Host

```
configure

domain ipv4 host host1 192.168.7.18
domain ipv4 host bost2 10.2.0.2 192.168.7.33
```

Defining the Domain Name

```
configure
domain name cisco.com
```

Specifying the Addresses of the Name Servers

```
configure

domain name-server 192.168.1.111
domain name-server 192.168.1.2
```

Configuring a Router to Use FTP or TFTP Connections: Example

The following example shows how to configure the router to use FTP or TFTP connections.

Using FTP

```
configure

ftp client passive
ftp client anonymous-password xxxx
ftp client source-interface HundredGigE 0/1/2/1
```

Using TFTP

```
configure
tftp client source-interface HundredGigE 1/0/2/1
```

Additional References

The following sections provide references related to implementing host services and addresses on .

Related Documents

Related Topic	Document Title
Host services and applications commands	*Host Services and Applications Commands* module in *IP Addresses and Services Command Reference for Cisco NCS 6000 Series Routers*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	Title
RFC-959	File Transfer Protocol
RFC-1738 and RFC-2732	Uniform Resource Locators (URL)
RFC-783	Trivial File Transfer Protocol

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport