



Kerberos Commands

This chapter describes the commands used to configure Kerberos. Kerberos is a secret-key network authentication protocol, developed at Massachusetts Institute of Technology (MIT), that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. Kerberos was designed to authenticate requests for network resources. Kerberos, like other secret-key systems, is based on the concept of a trusted third party that performs secure verification of users and services. In the Kerberos protocol, this trusted third party is called the key distribution center (KDC).

For information on how to configure Kerberos, refer to the “Configuring Kerberos” chapter in the *Security Configuration Guide*. For configuration examples using the commands in this chapter, refer to the “Kerberos Configuration Examples” section located at the end of the “Configuring Kerberos” chapter in the *Security Configuration Guide*.

clear kerberos creds

To delete the contents of the credentials cache, use the **clear kerberos creds** EXEC command.

clear kerberos creds

Syntax Description

This command has no keywords or arguments.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

Credentials are cleared when the user logs out.

Cisco supports Kerberos 5.

Example

The following example illustrates the **clear kerberos creds** command:

```
cisco-2500> show kerberos creds
Default Principal: chet@cisco.com
Valid Starting      Expires      Service Principal
18-Dec-1995 16:21:07 19-Dec-1995 00:22:24 krbtgt/CISCO.COM@CISCO.COM

cisco-2500> clear kerberos creds
cisco-2500> show kerberos creds
No Kerberos credentials.

cisco-2500>
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

show kerberos creds

connect

To log in to a host that supports Telnet, rlogin, or LAT, use the **connect** EXEC command.

connect *host* [*port*] [*keyword*]

Syntax Description

host A host name or an IP address.

port (Optional) A decimal TCP port number; the default is the Telnet router port (decimal 23) on the host.

keyword (Optional) One of the options listed in Table 9.

Table 9 describes the options that can be used for the argument *keyword*.

Table 9 Connection Options

Option	Description
/debug	Enables Telnet debugging mode.
/encrypt kerberos	Enables an encrypted Telnet session. This keyword is available only if you have the Kerberized Telnet subsystem. If you authenticate using Kerberos Credentials, the use of this keyword initiates an encryption negotiation with the remote server. If the encryption negotiation fails, the Telnet connection will be reset. If the encryption negotiation is successful, the Telnet connection will be established, and the Telnet session will continue in encrypted mode (all Telnet traffic for the session will be encrypted).
/line	Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press Return . You can edit the line using the standard Cisco IOS software command editing characters. The /line keyword is a local switch; the remote router is not notified of the mode change.
/noecho	Disables local echo.
/route path	Specifies loose source routing. The <i>path</i> argument is a list of host names or IP addresses that specify network nodes and ends with the final destination.
/source-interface	Specifies source interface.
/stream	Turns on <i>stream</i> processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UUCP and other non-Telnet protocols.
<i>port-number</i>	Port number.
bgp	Border Gateway Protocol.
chargen	Character generator.
cmd rcmd	Remote commands.
daytime	Daytime.
discard	Discard.
domain	Domain Naming Service.
echo	Echo.
exec	EXEC.

Table 9 Connection Options (Continued)

Option	Description
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections (used infrequently).
gopher	Gopher.
hostname	Network Information Center (NIC) host name server.
ident	Ident Protocol.
irc	Internet Relay Chat.
klogin	Kerberos login.
kshell	Kerberos shell.
login	Login (rlogin).
lpd	Printer service.
nntp	Network News Transport Protocol.
node	Connect to a specific LAT node.
pop2	Post Office Protocol v2.
pop3	Post Office Protocol v3.
port	Destination LAT port name.
smtp	Simple Mail Transport Protocol.
sunrpc	Sun Remote Procedure Call.
syslog	Syslog.
tacacs	Specify TACACS security.
talk	Talk.
telnet	Telnet.
time	Time.
uucp	UNIX-to-UNIX Copy Program.
whois	Nickname.
www	World Wide Web (HTTP).

Command Mode

EXEC

Usage Guidelines

This command first appeared in a release prior to Cisco IOS Release 10.0.

With the Cisco IOS software implementation of TCP/IP, you are not required to enter the **connect**, **telnet**, **lat**, or **rlogin** commands to establish a terminal connection. You can just enter the learned host name—as long as the host name is different from a command word in the Cisco IOS software.

To display a list of the available hosts, enter the following command:

show hosts

To display the status of all TCP connections, enter the following command:

show tcp

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

Examples

The following example establishes an encrypted Telnet session from a router to a remote host named *host1*:

```
Router> connect host1 /encrypt kerberos
```

The following example routes packets from the source system *host1* to *kl.sri.com*, then to *10.1.0.11*, and finally back to *host1*:

```
Router> connect host1 /route:kl.sri.com 10.1.0.11 host1
```

The following example connects to a host with logical name *host1*:

```
Router> host1
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

kerberos clients mandatory
lat

kerberos clients mandatory

To cause the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server, use the **kerberos clients mandatory** global configuration command. Use the **no** form of this command to disable this option.

kerberos clients mandatory
no kerberos clients mandatory

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

User Guidelines

This command first appeared in Cisco IOS Release 11.2.

If this command is not configured and the user has Kerberos credentials stored locally, the **rsh**, **rcp**, **rlogin**, and **telnet** commands attempt to negotiate the Kerberos protocol with the remote server and will use the non-Kerberized protocols if unsuccessful.

If this command is not configured and the user has no Kerberos credentials, the standard protocols for **rcp** and **rsh** are used to negotiate the Kerberos protocol.

Example

The following example causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server:

```
kerberos clients mandatory
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

copy rcp
kerberos credentials forward
rlogin
rsh
telnet

kerberos credentials forward

To force all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication, use the **kerberos credentials forward** global configuration command. Use the **no** form of this command to turn off Kerberos credentials forwarding.

kerberos credentials forward
no kerberos credentials forward

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Enable credentials forwarding to have users' TGTs forwarded to the host on which they authenticate. In this way, users can connect to multiple hosts in the Kerberos realm without running the KINIT program each time they need to get a TGT.

Example

The following example forces all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication:

```
kerberos credentials forward
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

copy rcp
rlogin
rsh
telnet

kerberos instance map

To map Kerberos instances to Cisco IOS privilege levels, use the **kerberos instance map** global configuration command. Use the **no** form of this command to remove a Kerberos instance map.

kerberos instance map *instance privilege-level*
no kerberos instance map *instance*

Syntax Description

<i>instance</i>	Name of a Kerberos instance.
<i>privilege-level</i>	The privilege level at which a user is set if the user's Kerberos principal contains the matching Kerberos instance. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges.

Default

Privilege level 1

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Use this command to create user instances with access to administrative commands.

Example

In the following example, the privilege level is set to 15 for authenticated Kerberos users with the *admin* instance in Kerberos realm:

```
kerberos instance map admin 15
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa authorization

kerberos local-realm

To specify the Kerberos realm in which the router is located, use the **kerberos local-realm** global configuration command. Use the **no** form of this command to remove the specified Kerberos realm from this router.

kerberos local-realm *kerberos-realm*
no kerberos local-realm

Syntax Description

<i>kerberos-realm</i>	The name of the default Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters.
-----------------------	---

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

The router can be located in more than one realm at a time. However, there can only be one instance of Kerberos local-realm. The realm specified with this command is the default realm.

Example

The following example specify the Kerberos realm in which the router is located as MURUGA.COM:

```
kerberos local-realm MURUGA.COM
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

kerberos preauth
kerberos realm
kerberos server
kerberos srvtab entry
kerberos srvtab remote

kerberos preauth

To specify a preauthentication method to use to communicate with the KDC, use the **kerberos preauth** global configuration command. Use the **no** form of this command to disable Kerberos preauthentication.

kerberos preauth [**encrypted-unix-timestamp** | **none**]
no kerberos preauth

Syntax Description

encrypted-unix-timestamp Use an encrypted UNIX timestamp as a quick authentication method when communicating with the KDC.

none Do not use Kerberos preauthentication.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

It is more secure to use a preauthentication for communications with the KDC. However, communication with the KDC will fail if the KDC does not support this particular version of **kerberos preauth**. If that happens, turn off the preauthentication with the **none** option.

The **no** form of this command is equivalent to using the **none** keyword.

Examples

The following example enables Kerberos preauthentication:

```
kerberos preauth encrypted-unix-timestamp
```

The following example disables Kerberos preauthentication:

```
kerberos preauth none
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

kerberos local-realm
kerberos server
kerberos srvtab entry
kerberos srvtab remote

kerberos realm

To map a host name or Domain Naming System (DNS) domain to a Kerberos realm, use the **kerberos realm** global configuration command. Use the **no** form of this command to remove a Kerberos realm map.

```
kerberos realm {dns-domain | host} kerberos-realm  
no kerberos realm {dns-domain | host} kerberos-realm
```

Syntax Description

<i>dns-domain</i>	Name of a DNS domain or host.
<i>host</i>	Name of a DNS host.
<i>kerberos-realm</i>	Name of the Kerberos realm to which the specified domain or host belongs.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

DNS domains are specified with a leading dot (.) character; host names cannot begin with a dot (.) character. There can be multiple entries of this line.

A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters. The router can be located in more than one realm at a time. Kerberos realm names must be in all uppercase characters.

Example

The following example maps the domain name, muruga.com, to the Kerberos realm, MURUGA.COM:

```
kerberos realm .muruga.com MURUGA.COM  
kerberos realm muruga.com MURUGA.COM
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

kerberos local-realm

kerberos server

kerberos srvtab entry

kerberos srvtab remote

kerberos server

To specify the location of the Kerberos server for a given Kerberos realm, use the **kerberos server** global configuration command. Use the **no** form of this command to remove a Kerberos server for a specified Kerberos realm.

kerberos server *kerberos-realm* {*hostname* | *ip-address*} [*port-number*]
no kerberos server *kerberos-realm* {*hostname* | *ip-address*}

Syntax Description

<i>kerberos-realm</i>	Name of the Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase letters.
<i>hostname</i>	Name of the host functioning as a Kerberos server for the specified Kerberos realm (translated into an IP address at the time of entry).
<i>ip-address</i>	IP address of the host functioning as a Kerberos server for the specified Kerberos realm.
<i>port-number</i>	(Optional) Port that the KDC/TGS monitors (defaults to 88).

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

Example

The following example specifies 192.168.47.66 as the Kerberos server for the Kerberos realm MURUGA.COM:

```
kerberos server MURUGA.COM 192.168.47.66
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

kerberos local-realm
kerberos realm
kerberos srvtab entry
kerberos srvtab remote

kerberos srvtab entry

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the **kerberos srvtab remote** global configuration command (not **kerberos srvtab entry**). (The Kerberos SRVTAB entry is the router's locally stored SRVTAB.) Use the **no** form of this command to remove a SRVTAB entry from the router's configuration.

```
kerberos srvtab entry kerberos-principal principal-type timestamp key-version number
                        key-type key-length encrypted-keytab
no kerberos srvtab entry kerberos-principal principal-type
```

Syntax Description

<i>kerberos-principal</i>	A service on the router.
<i>principal-type</i>	Version of the Kerberos SRVTAB.
<i>timestamp</i>	Number representing the date and time the SRVTAB entry was created.
<i>key-version number</i>	Version of the encryption key format.
<i>key-type</i>	Type of encryption used.
<i>key-length</i>	Length, in bytes, of the encryption key.
<i>encrypted-keytab</i>	Secret key the router shares with the KDC. It is encrypted with the private Data Encryption Standard (DES) key (if available) when you write out your configuration.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

When you use the **kerberos srvtab remote** command to copy the SRVTAB file from a remote host (generally the KDC), it parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry** format. The key for each SRVTAB entry is encrypted with a private DES key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the **write memory** router configuration command to write the router's running configuration to NVRAM.

If you reload a configuration, with a SRVTAB encrypted with a private DES key, on to a router that does not have a private DES key defined, the router displays a message informing you that the SRVTAB entry has been corrupted, and discards the entry.

If you change the private DES key and reload an old version of the router's configuration that contains SRVTAB entries encrypted with the old private DES keys, the router will restore your Kerberos SRVTAB entries, but the SRVTAB keys will be corrupted. In this case, you must delete your old Kerberos SRVTAB entries and reload your Kerberos SRVTABs on to the router using the **kerberos srvtab remote** command.

Although you can configure **kerberos srvtab entry** on the router manually, generally you would not do this because the keytab is encrypted automatically by the router when you copy the SRVTAB using the **kerberos srvtab remote** command.

Example

In the following example, host/new-router.loki.com@LOKI.COM is the host, 0 is the type, 817680774 is the timestamp, 1 is the version of the key, 1 indicates the DES is the encryption type, 8 is the number of bytes, and .cCN.YoU.okK is the encrypted key:

```
kerberos srvtab entry host/new-router.loki.com@LOKI.COM 0 817680774 1 1 8 .cCN.YoU.okK
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

kerberos srvtab remote
key config-key

kerberos srvtab remote

To retrieve a krb5 SRVTAB file from the specified host, use the **kerberos srvtab remote** global configuration command.

kerberos srvtab remote {*hostname* | *ip-address*} *filename*

Syntax Description

<i>hostname</i>	Machine with the Kerberos SRVTAB file.
<i>ip-address</i>	IP address of the machine with the Kerberos SRVTAB file.
<i>filename</i>	Name of the SRVTAB file.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

When you use the **kerberos srvtab remote** command to copy the SRVTAB file from the remote host (generally the KDC), it parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry** format. The key for each SRVTAB entry is encrypted with the private Data Encryption Standard (DES) key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the **write memory** configuration command to write the router's running configuration to NVRAM.

Example

The command in the following example copies the SRVTAB file residing on bucket.cisco.com to a router named scooter.cisco.com:

```
kerberos srvtab remote bucket.cisco.com scooter.cisco.com-new-srvtab
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

kerberos srvtab entry
key config-key

key config-key

To define a private DES key for the router, use the **key config-key** global configuration command. Use the **no** form of this command to delete a private DES key for the router.

key config-key 1 *string*

Syntax Description

string Private DES key (can be up to eight alphanumeric characters).

Default

No DES-key defined

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

This command defines a private DES key for the router that will not show up in the router configuration. This private DES key can be used to DES-encrypt certain parts of the router's configuration.



Caution The private DES key is unrecoverable. If you encrypt part of your configuration with the private DES key and lose or forget the key, you will not be able to recover the encrypted data.

Example

The command in the following example sets *bubba* as the private DES key on the router:

```
key config-key 1 bubba
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

kerberos srvtab entry

kerberos srvtab remote

show kerberos creds

To display the contents of your credentials cache, use the **show kerberos creds** EXEC command.

show kerberos creds

Syntax Description

This command has no keywords or arguments.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

The **show kerberos creds** command is equivalent to the UNIX klist command.

When users authenticate themselves with Kerberos, they are issued an authentication ticket called a *credential*. The credential is stored in a credential cache.

Sample Displays

In the following example, the entries in the credentials cache are displayed:

```
Router> show kerberos creds

Default Principal: chet@cisco.com
Valid Starting      Expires      Service Principal
18-Dec-1995 16:21:07 19-Dec-1995 00:22:24  krbtgt/CISCO.COM@CISCO.COM
```

In the following example, output is returned that acknowledges that credentials do *not* exist in the credentials cache:

```
Router> show kerberos creds

No Kerberos credentials
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

clear kerberos creds

telnet

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

telnet *host* [*port*] [*keyword*]

Syntax Description

host A host name or an IP address.

port (Optional) A decimal TCP port number; the default is the Telnet router port (decimal 23) on the host.

keyword (Optional) One of the options listed in Table 10.

Table 10 describes the options that can be used for the argument *keyword*.

Table 10 Telnet Connection Options

Option	Description
/debug	Enables Telnet debugging mode.
/encrypt kerberos	Enables an encrypted Telnet session. This keyword is available only if you have the Kerberized Telnet subsystem. If you authenticate using Kerberos Credentials, the use of this keyword initiates an encryption negotiation with the remote server. If the encryption negotiation fails, the Telnet connection will be reset. If the encryption negotiation is successful, the Telnet connection will be established, and the Telnet session will continue in encrypted mode (all Telnet traffic for the session will be encrypted).
/line	Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press Return . You can edit the line using the standard Cisco IOS software command-editing characters. The /line keyword is a local switch; the remote router is not notified of the mode change.
/noecho	Disables local echo.
/route path	Specifies loose source routing. The <i>path</i> argument is a list of host names or IP addresses that specify network nodes and ends with the final destination.
/source-interface	Specifies source interface.
/stream	Turns on <i>stream</i> processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UUCP and other non-Telnet protocols.
<i>port-number</i>	Port number.
bgp	Border Gateway Protocol.
chargen	Character generator.
cmd rcmd	Remote commands.
daytime	Daytime.
discard	Discard.
domain	Domain Name System.
echo	Echo.
exec	EXEC.

Table 10 Telnet Connection Options (Continued)

Option	Description
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections (used infrequently).
gopher	Gopher.
hostname	NIC hostname server.
ident	Ident Protocol.
irc	Internet Relay Chat
klogin	Kerberos login.
kshell	Kerberos shell.
login	Login (rlogin).
lpd	Printer service.
nntp	Network News Transport Protocol.
node	Connect to a specific LAT node.
pop2	Post Office Protocol v2.
pop3	Post Office Protocol v3.
port	Destination LAT port name.
smtp	Simple Mail Transport Protocol.
sunrpc	Sun Remote Procedure Call.
syslog	Syslog.
tacacs	Specify TACACS security.
talk	Talk.
telnet	Telnet.
time	Time.
uucp	UNIX-to-UNIX Copy Program.
whois	Nickname.
www	World Wide Web (HTTP).

Command Mode

EXEC

Usage Guidelines

This command first appeared in a release prior to Cisco IOS Release 10.0.

With the Cisco IOS implementation of TCP/IP, you are not required to enter the **connect** or **telnet** commands to establish a Telnet connection. You can just enter the learned host name—as long as the following conditions are met:

- The host name is different from a command word for the router
- The preferred transport protocol is set to Telnet

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

The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is Ctrl-^ (press and hold the Control and Shift keys and the 6 key). You can enter the command character as you hold down Ctrl or with Ctrl released; you can use either uppercase or lowercase letters. Table 11 lists the special Telnet escape sequences.

Table 11 Special Telnet Escape Sequences

Task	Escape Sequence ¹
Break	Ctrl-^ b
Interrupt Process (IP)	Ctrl-^ c
Erase Character (EC)	Ctrl-^ h
Abort Output (AO)	Ctrl-^ o
Are You There? (AYT)	Ctrl-^ t
Erase Line (EL)	Ctrl-^ u

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

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

Ctrl-^ ?

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

```
Router> ^^?  
[Special telnet escape help]  
^^B  sends telnet BREAK  
^^C  sends telnet IP  
^^H  sends telnet EC  
^^O  sends telnet AO  
^^T  sends telnet AYT  
^^U  sends telnet EL
```

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

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

close
disconnect
exit
logout
quit

Examples

The following example establishes an encrypted Telnet session from a router to a remote host named *host1*:

```
Router> telnet host1 /encrypt kerberos
```

The following example routes packets from the source system *host1* to *kl.sri.com*, then to *10.1.0.11*, and finally back to *host1*:

```
Router> telnet host1 /route:kl.sri.com 10.1.0.11 host1
```

The following example connects to a host with logical name *host1*:

```
Router> host1
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

connect
rlogin

