Terminal Services Commands

absolute-timeout

To set the interval for closing the connection, use the **absolute-timeout** command in line configuration mode. To restore the default, use the **no** form of this command.

absolute-timeout *minutes*

no absolute-timeout

Syntax Description

minutes	Number of minutes after which the user session will be terminated.

Defaults

No timeout interval is automatically set.

Command Modes

Line configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **absolute-timeout** command line configuration command to configure the EXEC to terminate when the configured number of minutes occurs on the virtual terminal (vty) line. The **absolute-timeout** command terminates the connection after the specified time period has elapsed, regardless of whether the connection is being used at the time of termination. You can specify an absolute-timeout value for each port. The user is given 20 seconds notice before the session is terminated. You can use this command along with the **logout-warning** command to notify users of an impending logout.

Cisco IOS software also provides the **session-timeout** and **exec-timeout** line configuration commands for releasing lines when they have been idle for too long.

You can set the **absolute-timeout** command and an AppleTalk Remote Access Protocol (ARAP) timeout for the same line; however, this command supersedes any timeouts set in ARAP. Additionally, ARAP users will receive no notice of any impending termination if you use this command.

Examples

The following example sets an interval of 60 minutes on line 5:

```
line 5
 absolute-timeout 60
```

Related Commands

Command	Description
exec-timeout	Sets the interval that the EXEC command interpreter waits until user input is detected.
logout-warning	Sets and displays a warning for users about an impending forced timeout.
session-timeout	Sets the interval for closing the connection on a console or terminal line.

access-class (LAT)

To define restrictions on incoming and outgoing connections, use the **access-class** command in line configuration mode. To remove the access list number, use the **no** form of this command.

access-class *access-list-number* {**in** [**vrf-also**] | **out**}

no access-class *access-list-number* {**in** | **out**}

Syntax Description

access-list-number	Specifies an integer from 1 to 199 that defines the access list.
in	Controls which nodes can make local-area transport (LAT) connections into the server.
vrf-also	(Optional) Accepts incoming connections from interfaces that belong to a VRF.
out	Defines the access checks made on outgoing connections. (A user who types a node name at the system prompt to initiate a LAT connection is making an outgoing connection.)

Defaults

Disabled

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The **vrf-also** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command defines access list numbers that will then be used with the **lat access-list** command to specify the access conditions.

The value supplied for the *access-list-number* argument is used for all protocols supported by the Cisco IOS software. If you are already using an IP access list, you must define LAT and possibly X.25 access lists permitting connections to all devices, to emulate the behavior of previous software versions.

When both IP and LAT connections are allowed from a terminal line and an IP access list is applied to that line with the **access-class** line configuration command, you must also create a LAT access list with the same number if you want to allow any LAT connections from that terminal. You can specify only one incoming and one outgoing access list number for each terminal line.When checking LAT access lists, if the specified list does not exist, the system denies all LAT connections.

If you do not specify the **vrf-also** keyword, incoming Telnet connections from interfaces that are part of a VRF are rejected.

Examples

The following example configures an incoming access class on vty line 4:

```
line vty 4
 access-class 4 in
```

Related Commands

Command	Description
lat access-list	Specifies access conditions to nodes on the LAT network.

arap dedicated

To configure a line to be used only as an AppleTalk Remote Access (ARA) connection, use the **arap dedicated** command in line configuration mode. To return the line to interactive mode, use the **no** form of this command.

arap dedicated

no arap dedicated

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures line 3 to be used only for ARA connections:

```
line 3
 arap dedicated
```

arap enable

To enable AppleTalk Remote Access (ARA) for a line, use the **arap enable** command in line configuration mode. To disable ARA, use the **no** form of this command.

arap enable

no arap enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables ARA on line 3:

```
line 3
 arap enable
```

Related Commands

Command	Description
appletalk routing	Enables AppleTalk routing.
autoselect	Configures a line to start an ARA, PPP, or SLIP session.

arap net-access-list

To control Apple Macintosh access to networks, use the **arap net-access-list** command in line configuration mode. To return to the default setting, use the **no** form of this command.

arap net-access-list *net-access-list-number*

no arap net-access-list *net-access-list-number*

Syntax Description

net-access-list-number	One of the *list* values configured using the AppleTalk **access-list cable-range**, **access-list includes**, **access-list network**, **access-list other-access**, or **access-list within** commands.

Defaults

Disabled. The Macintosh has access to all networks.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can use the **arap net-access-list** command to apply access lists defined by the **access-list cable-range**, **access-list includes**, **access-list network**, **access-list other-access**, or **access-list within** commands.

You cannot use the **arap net-access-list** command to apply access lists defined by the **access-list zone** or **access-list additional-zones** commands.

Examples

In the following example, ARA is enabled on line 3 and the Macintosh will have access to the AppleTalk access list numbered 650:

```
line 3
 arap enable
 arap net-access-list 650
```

Related Commands

Command	Description
access-list cable-range	Defines an AppleTalk access list for a cable range (for extended networks only).
access-list includes	Defines an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks).
access-list network	Defines an AppleTalk access list for a single network number (that is, for a nonextended network).
access-list other-access	Defines the default action to take for subsequent access checks that apply to networks or cable ranges.
access-list within	Defines an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range.
arap zonelist	Controls which zones the Apple Macintosh client sees.

arap network

To create a new network or zone and cause it to be advertised, use the **arap network** command in global configuration mode. To prevent a new network or zone from being advertised, use the **no** form of this command.

arap network [*network-number*] [*zone-name*]

no arap network

Syntax Description

network-number	(Optional) AppleTalk network number. The network number must be unique on your AppleTalk network. This network is where all AppleTalk Remote Access (ARAP) users appear when they dial in to the network.
zone-name	(Optional) AppleTalk zone name.

Defaults

A new network or zone is not created.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This is a required command. ARAP does not run without it in Cisco IOS Release 10.2 and later.

Examples

The following example creates a new zone named test zone:

```
arap network 400 test zone
```

arap require-manual-password

To require users to enter their password manually at the time they log in, use the **arap require-manual-password** command in line configuration mode. To disable the manual password-entry requirement, use the **no** form of this command.

arap require-manual-password

no arap require-manual-password

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Line configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command only works for AppleTalk Remote Access Protocol (ARAP) 2.0 connections.

Examples

The following example forces users to enter their passwords manually at the time they log in, rather than use a saved password:

```
arap require-manual-password
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
login (line)	Enables password checking at login and defines the method (local or TACACS+).
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.

arap timelimit

To set the maximum length of an AppleTalk Remote Access (ARA) session for a line, use the **arap timelimit** command in line configuration mode. To return to the default of unlimited session length, use the **no** form of this command.

arap timelimit [*minutes*]

no arap timelimit

Syntax Description

minutes	(Optional) Maximum length of time, in minutes, for a session.

Defaults

Unlimited session length

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

After the specified length of time, the session will be terminated.

Examples

The following example specifies a maximum length of 20 minutes for ARA sessions:

```
line 3
 arap enable
 arap timelimit 20
```

Related Commands

Command	Description
arap warningtime	Sets when a disconnect warning message is displayed.

arap warningtime

To set when a disconnect warning message is displayed, use the **arap warningtime** command in line configuration mode. To disable this function, use the **no** form of this command.

arap warningtime [*minutes*]

no arap warningtime

Syntax Description

minutes	(Optional) Amount of time, in minutes, before the configured session time limit. At the configured amount of time before a session is to be disconnected, the router sends a message to the Apple Macintosh client, which causes a warning message to appear on the user screen.

Defaults

Disabled

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command can only be used if a session time limit has been configured on the line.

Examples

The following example shows a line configured for 20-minute AppleTalk Remote Access (ARA) sessions, with a warning 17 minutes after the session is started:

```
line 3
 arap enable
 arap dedicated
 arap timelimit 20
 arap warningtime 3
```

Related Commands

Command	Description
arap timelimit	Sets the maximum length of an ARA session for a line.

arap zonelist

To control which zones the Apple Macintosh client sees, use the **arap zonelist** command in line configuration mode. To disable the default setting, use the **no** form of this command.

arap zonelist *zone-access-list-number*

no arap zonelist *zone-access-list-number*

Syntax Description

zone-access-list-number	One of the *list* values configured using the AppleTalk **access-list zone** or **access-list additional-zones** command.

Defaults

Disabled. The Macintosh will see all defined zones.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can use the **arap zonelist** command to apply access lists defined by the **access-list zone** and **access-list additional-zones** commands.

You cannot use the **arap zonelist** command to apply access lists defined by the **access-list network** command.

Hiding a zone from users is not the same as preventing them from sending and receiving packets from the networks that make up that zone. For true security, an **arap net-access-list** command must be issued to prevent traffic to and from those networks.

Examples

The following example enables AppleTalk Remote Access (ARA) on line 3; the Macintosh will see only zones permitted by access list 650.

```
line 3
 arap enable
 arap zonelist 650
```

Related Commands

Command	Description
access-list additional-zones	Defines the default action to take for access checks that apply to zones.

Command	Description
access-list zone	Defines an AppleTalk access list that applies to a zone.
arap net-access-list	Controls Apple Macintosh access to networks.

async default ip address

The **async default ip address** command is replaced by the **peer default ip address** command. See the **peer default ip address** command for more information.

authentication-retries

To specify the number of authentication retries before dropping the connection for a persistent Secure Shell (SSH) connection attempt, use the **authentication-retries** transport map configuration mode command. To restore the default setting of three retries, use the **no** form of the command.

authentication-retries *number-of-retries*

no authentication-retries

Syntax Description

number-of-retries	Specifies the number of retries before the connection attempt is dropped.

Command Default

The default *number-of-retries* is 3.

Command Modes

Transport map configuration (config-tmap)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

This command configures the number of authentication retries for users using SSH to connect to a Management Ethernet interface with an applied transport map.

Examples

In the following example, a transport map is configured that will apply the following settings to any users attempting to access the Management Ethernet port via SSH:

- Users using SSH wait for the IOS process to become active, but enter diagnostic mode if the attempt to access IOS is interrupted.
- The RSA keypair name is "sshkeys".
- The connection allows one authentication retry.
- The banner "--Welcome to Diagnostic Mode--" appears if diagnostic mode is entered as a result of SSH handling through this transport map.
- The banner "--Waiting for IOS Process--" appears if the connection is waiting for the IOS process to be come active.

The transport map is then applied to the interface when the **transport type persistent ssh input** command is entered to enable persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# authentication-retries 1
Router(config-tmap)# banner diagnostic X
Enter TEXT message.  End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message.  End with the character 'X'.
--Waiting for IOS Process--
X
Router(config-tmap)# time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit

Router(config)# transport type persistent ssh input sshhandler
```

Related Commands

Command	Description
banner (transport map)	Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the transport map configuration.
connection wait	Specifies how an incoming connection will be handled.
rsa keypair-name	Names the RSA keypair to be used for persistent SSH connections.
time-out	Specifies the SSH timeout interval in seconds.
transport interface	Applies the transport map settings to the interface.
transport type persistent	Applies an already-configured persistent transport map to an interface.
transport-map type persistent	Creates and names a persistent transport map and enters transport map configuration mode.

autocommand

To configure the system to automatically execute a specific EXEC command when it connects to a port, use the **autocommand** command in line configuration mode. To disable the automatic execution, use the **no** form of this command.

autocommand [**no-suppress-linenumber**] *command-text*

no autocommand

Syntax Description

no-suppress-linenumber	Displays the service line number for which the EXEC commands are automatically executed.
command-text	Any appropriate EXEC command, including the host name and any switches that must be used with the EXEC command.

Defaults

No commands are configured to automatically execute.

Command Modes

Line configuration (config-line)

Command History

Release	Modification
10.0	This command was introduced.
12.0T	The **no-suppress-linenumber** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The line number message enables users to track the port that is currently connected. The line numbers for these messages are provided by the **service linenumber** command. The **autocommand** command generally suppresses the line number message. However, when **autocommand** is used with the **no-suppress-linenumber** keyword, the line number messages are not suppressed.

Examples

The following example shows how to force an automatic connection to host21:

```
Router(config)# line vty 4
Router(config-line)# autocommand no-suppress-linenumber connect host21
Router(config-line)#
```

Related Commands

Command	Description
service linenumber	Configures Cisco IOS software to display line number information after the EXEC or incoming banner.

banner (transport map)

To create a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of a transport map configuration configured on a console port or for users using Telnet or Secure Shell (SSH), use the **banner** command in transport map configuration mode. To restore the default setting of no diagnostic or no wait banner, use the **no** form of the command.

banner [**diagnostic** | **wait**] *banner-message*

no banner [diagnostic | wait]

Syntax Description

diagnostic	Creates a banner message seen by users directed into diagnostic mode as a result of the transport map handling of the connection.
wait	Creates a banner message seen by users waiting for the IOS mode to become active as a result of the transport map handling of the connection.
banner-message	The banner message, which begins and ends with the same delimiting character.

Command Default

There are no banners configured for transport maps by default.

Command Modes

Transport map configuration (config-tmap)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

Configuring the diagnostic and wait banners is optional but recommended. The banners are especially useful as indicators to users of the status of their Telnet, SSH, or console port connection attempts.

When defining the *banner-message*, it is advisable to press **Enter** before entering the final delimiting character. Pressing **Enter** moves the cursor down a line and ensures the prompt on the router does not appear on the same line as the banner when the banner posts during a Telnet or SSH session.

The currently applied banner messages can be checked using the **show platform software configuration access policy** command.

Examples

In the following example, a transport map that will make all Telnet connections wait for the IOS process to become active before connecting to the router, while also allowing the user to interrupt the process and enter diagnostic mode, is configured and applied to the Management Ethernet interface (interface gigabitethernet 0).

A diagnostic and a wait banner are also configured.

The transport map is then applied to the interface when the **transport type persistent telnet input** command is entered to enable persistent Telnet.

```
Router(config)# transport-map type persistent telnet telnethandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# banner diagnostic X
Enter TEXT message.  End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message.  End with the character 'X'.
--Waiting for IOS Process--
X

Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

In the following example, a transport map to set console port access policies is created and attached to console port 0. The transport map configuration includes both a diagnostic and a wait banner.

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# banner diagnostic X
Enter TEXT message.  End with the character 'X'.
Welcome to diagnostic mode
X
Router(config-tmap)# banner wait X
Enter TEXT message.  End with the character 'X'.
Waiting for IOS prompt
X
Router(config-tmap)# exit

Router(config)# transport type console 0 input consolehandler
```

Related Commands

Command	Description
authentication-retries	Specifies the number of SSH authentication retries before dropping the connection when a persistent SSH transport map is applied to the receiving interface.
connection wait	Specifies how an incoming connection will be handled.
rsa keypair-name	Names the RSA keypair to be used for persistent SSH connections.
show platform software configuration access policy	Displays the access policy and banner settings for console, Telnet, and SSH connections.
time-out	Specifies the SSH timeout interval in seconds.
transport interface	Applies the transport map settings to the interface.
transport type persistent	Applies an already-configured persistent transport map to an interface.
transport-map type persistent	Creates and names a persistent transport map and enters transport map configuration mode.

busy-message

To create a "host failed" message that displays when a connection fails, use the **busy-message** command in global configuration mode. To disable the "host failed" message from displaying on the specified host, use the **no** form of this command.

busy-message *host-name d message d*

no busy-message *host-name*

Syntax Description

host-name	Name of the host that cannot be reached.
d	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the message.
message	Message text.

Defaults

No message is displayed.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies only to Telnet connections.

Follow the **busy-message** command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Defining a "host failed" message for a host prevents all Cisco IOS software-initiated user messages, including the initial message that indicates the connection is "Trying...." The **busy-message** command can be used in the **autocommand** command to suppress these messages.

Examples

The following example sets a message that will be displayed on the terminal whenever an attempt to connect to the host named router1 fails. The pound sign (#) is used as a delimiting character.

```
busy-message router1 #
Cannot connect to host. Contact the computer center.
#
```

Related Commands

Command	Description
autocommand	Automatically execute a command when a user connects to a particular line.

clear entry

To delete an entry from the list of queued host-initiated connections, use the **clear entry** command in EXEC mode.

clear entry *number*

Syntax Description

number	An entry number obtained from the **show entry** EXEC command.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example deletes pending entry number 3 from the queue:

```
Router# clear entry 3
```

Related Commands

Command	Description
show entry	Displays the list of queued host-initiated connections to a router.

connect

To log in to a host that supports Telnet, rlogin, or local-area transport (LAT), use the **connect** command in EXEC mode.

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 keywords listed in Table 1.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced in a release prior to Cisco IOS Release 10.0.
12.0(21)ST	The **/ipv4** and **/ipv6** keywords were added.
12.1	The **/quiet** keyword was added.
12.2(2)T	Support for the **/ipv4** and **/ipv6** keywords was integrated into Cisco IOS Release 12.2(2)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Table 1 lists the optional **connect** command keywords.

Table 1 connect Keyword 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).
/ipv4	Forces the use of IP version 4.
/ipv6	Forces the use of IP version 6.

Table 1 connect Keyword Options (continued)

Option	Description
/line	Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press the Enter key. 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.
/quiet	Prevents onscreen display of all messages from the Cisco IOS software.
/route *path*	Specifies loose source routing. The *path* argument is a list of host names or IP addresses that specify network nodes and ends with the final destination.
/source-interface	Specifies the source interface.
/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.
bgp	Border Gateway Protocol.
chargen	Character generator.
cmd *rcmd*	Remote commands.
daytime	Daytime.
discard	Discard.
domain	Domain Naming Service.
echo	Echo.
exec	EXEC.
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections (used infrequently).
gopher	Gopher.
hostname	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.
port-number	Port number.

Table 1 connect Keyword Options (continued)

Option	Description
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.

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 enter only the learned host name—as long as the host name is different from a command word in the Cisco IOS software. 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. 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.

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 named host1 to router1.cisco.com, then to 10.1.0.11, and finally back to host1:

```
Router> connect host1 /route:router1.cisco.com 10.1.0.11 host1
```

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

```
Router> host1
```

The following example suppresses all onscreen messages from the Cisco IOS software during login and logout:

```
Router> connect host2 /quiet
```

The following example shows the limited messages displayed when connection is done using the optional **/quiet** keyword:

```
login:User2

Password:
         Welcome to OpenVMS VAX version V6.1 on node CRAW
     Last interactive login on Tuesday, 15-DEC-1998 11:01
     Last non-interactive login on Sunday,  3-JAN-1999 22:32
```

```
Server3)logout

User2        logged out at  16-FEB-2000 09:38:27.85
```

Related Commands

Command	Description
kerberos clients mandatory	Causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos Protocol with the remote server.
l2f ignore-mid-sequence	Specifies a connection to a particular LAT node that offers LAT services.
lat	Connects to a LAT host.
name-connection	Assigns a logical name to a connection.
rlogin	Logs in to a UNIX host using rlogin.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.
show tcp	Displays the status of TCP connections.
telnet	Logs in to a host that supports Telnet.

connection wait

To specify how users accessing a router using Telnet, Secure Shell (SSH), or the console port will be connected, use the **connection wait** command in transport map configuration mode. To restore the default setting of waiting for an IOS vty line to become available while also allowing the user to enter diagnostic mode if the connection that is waiting for the IOS vty line is interrupted, use the **no** or **default** form of the command.

connection wait [**allow** [**interruptable**]| **none** [**disconnect**]]

no connection wait [**allow** [**interruptable**]| **none** [**disconnect**]]

Syntax Description

allow	Specifies the Telnet or SSH connection will wait for the IOS process to become available, and will exit the router if interrupted. This option is not available for console port transport maps.
allow interruptable	Specifies the Telnet, SSH, or console port connection will wait for the IOS process to become available, and also will allow users to enter diagnostic mode by interrupting a Telnet connection waiting for the IOS process to become available.
none	Specifies the Telnet, SSH, or console port connection immediately enters diagnostic mode.
none disconnect	Specifies the Telnet or SSH connection will not wait for the IOS process and will not enter diagnostic mode, so all Telnet or SSH connections are rejected. This option is not available for console port transport maps.

Command Default

The default connection setting is **allow interruptable**.

Command Modes

Transport map configuration (config-tmap)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

When **connection wait allow interruptable** is configured, users enter diagnostic mode by sending a break signal while waiting to connect to the IOS process. The **Ctrl-C** or **Ctrl-Shift-6** sequences are used to send a break signal.

For a persistent Telnet connection to access IOS on the Cisco ASR 1000 Series Routers, local login authentication must be configured for the vty line (the **login** command in line configuration mode). If local login authentication is not configured, users will not be able to access IOS using a Telnet connection into the Management Ethernet interface with an applied transport map. Diagnostic mode will still be accessible in this scenario.

Examples

In the following example, a transport map that makes all Telnet connections wait for the IOS vty line to become active before connecting to the router, while also allowing the user to interrupt the process and enter diagnostic mode, is configured and applied to the Management Ethernet interface (interface gigabitethernet 0).

A diagnostic and a wait banner are also configured.

The transport map is then applied to the interface when the **transport type persistent telnet input** command is entered to enable persistent Telnet.

```
Router(config)# transport-map type persistent telnet telnethandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# banner diagnostic X
Enter TEXT message.  End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message.  End with the character 'X'.
--Waiting for IOS Process--
X

Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

In the following example, a transport map to set console port access policies is created and attached to console port 0.

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# banner diagnostic X
Enter TEXT message.  End with the character 'X'.
Welcome to diagnostic mode
X
Router(config-tmap)# banner wait X
Enter TEXT message.  End with the character 'X'.
Waiting for IOS prompt
X
Router(config-tmap)# exit

Router(config)# transport type console 0 input consolehandler
```

Related Commands

Command	Description
authentication-retries	Specifies the number of SSH authentication retries before dropping the connection when a persistent SSH transport map is applied to the receiving interface.
banner (transport map)	Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the transport map configuration.
rsa keypair-name	Names the RSA keypair to be used for persistent SSH connections.
show platform software configuration access policy	Displays the access policy and banner settings for console, Telnet, and SSH connections.
time-out	Specifies the SSH timeout interval in seconds.
transport interface	Applies the transport map settings to the interface.

Command	Description
transport type persistent	Applies an already-configured persistent transport map to an interface.
transport-map type persistent	Creates and names a persistent transport map enters transport map configuration mode.

description (ruleset)

To add a description about a translation ruleset, use the **description** command in translate ruleset configuration mode. To remove the description, use the **no** form of this command.

description *text*

no description *text*

Syntax Description

text	One-line description of the ruleset, up to 240 characters.

Defaults

No default behavior or values

Command Modes

Translate ruleset configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Only one description line is accepted. If you reenter this command, the new description replaces the existing description.

Examples

The following example shows how to add a description to a ruleset:

```
translate ruleset A from pad to telnet
 description Template A for site 101
 skip dest-addr ^55554$ source-addr ^4444$
 match dest-addr ^5555.$ source-addr ^4444$
 set telnet dest-addr 10.2.2.1
 substitute pad dest-addr ^5555(.) into telnet dest-port 23
```

Related Commands

Command	Description
match (ruleset)	Identifies a connection for processing by the translation ruleset.
options (ruleset)	Specifies protocol translation options in a translation ruleset.
set (ruleset)	Unconditionally sets one or more connection parameters to a fixed value for a translation ruleset.
show translate ruleset	Displays a summary of a specific or of all configured translation rulesets, behavioral parameters, and usage statistic.
skip (ruleset)	Identifies a connection for omission by the translation ruleset.

Command	Description
substitute (ruleset)	Matches an available protocol and substitutes another in a translation ruleset.
test (ruleset)	Tests parameter values in a translation ruleset using regular expressions.
test translate	Displays a trace of protocol translation behavior for a connection attempt.
translate ruleset	Defines a unique name for a translation ruleset, specifies translated protocols, and enters translate ruleset configuration mode.
x25 pvc translate ruleset	Configures PVCs that are valid for protocol translation rule set handling.

flush-at-activation

To discard any data or noise characters that are sitting in the input buffer of the asynchronous line before the line is activated, use the **flush-at-activation** command in line configuration mode. To keep any data or noise characters that are sitting in the input buffer of the asynchronous line before the line is activated, use the **no** form of this command.

flush-at-activation

no flush-at-activation

Syntax Description

This command has no keywords or arguments.

Defaults

Enabled by default.

Command Modes

Line configuration

Command History

Release	Modification
11.1(5)	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For an incoming call on a line configured with modem control (using the **modem inout** and **modem dialin** commands), the line will be activated when the data set ready (DSR) signal goes high and will be dropped when the DSR signal goes low. While the line is idle, its input buffer may receive characters; for example, modem result codes such as "NO CARRIER" or "RING" or line noise. Such characters are not useful to the line application. Flushing the line input buffer when the DSR goes high using the **flush-at-activation** command is the preferred behavior.

Note To know whether the DSR signal is going high or low, use the **debug modem** command or the **show line** command. Output of these commands displays the status of DSR signal.

On most Cisco IOS platforms, there may be up to a one-second delay between when the DSR signal goes high and Cisco IOS activates the line. Therefore, some valid data received from the line may be discarded when you issue the **flush-at-activation command**. If it is important to process this valid data rather than discarding it and the application is tolerant of receiving bad data, configure the **no flush-at-activation** command.

The application that is used determines whether the system can differentiate the valid data from the bad data or the system is tolerant of receiving any data. For example, consider that the application used is TCP over IP over PPP. PPP uses a Frame Check Sequence (FCS) in a data frame format to verify the integrity of the received data. If an invalid data pattern is delivered to a PPP receiver, PPP will discard it as a framing or FCS error. So the bad data will not be delivered to the higher layers. Even if some data is delivered up to IP and TCP, TCP has its own FCS which will reject bad data. Therefore, the application is tolerant of receiving the bad data that the line delivers.

Consider another application where incoming character data received from the line is delivered as TCP payload to a server running a pager application. Unless the pager application has implemented its own protocol to verify data integrity, this bad data may cause the pager not to be delivered, or to deliver bad data within the message payload to the receiving pager. So the bad data should not be delivered as payload to the line.

Where an upper-layer framed protocol such as PPP or Serial Line Internet Protocol (SLIP) is always used (asynchronous mode dedicated), the framed protocol may reach link status more quickly when you issue the **no flush-at-activation** command. Since the framed protocol discards any erroneous data received, you do not have to use the **flush-at-activation** command.

If the line application is not tolerant of receiving bad data; for example, when you are using character-mode username/password authentication, always use the **flush-at-activation** command. Otherwise, the bad data may trigger an application failure.

Note Prior to Cisco IOS Release 12.2, the **no flush-at-activation** command was the default on AS5000 platforms with modem ISDN channel aggregation (MICA) and NextPort modems. However, from Cisco IOS Release 12.3 and later, there is no longer any significant delay between when the modem link reaches steady state (DSR high) and when the line is activated so you do not need to use the **no flush-at-activation** command.
The modem state STEADY_STATE is mapped to DSR high and TERMINATING is mapped to DSR low when asynchronous lines are the internal digital modem ports.

Examples

The following example shows how to configure lines 1/0 through 1/59 to flush any data in their input buffers when the lines are activated:

```
Router(config)# line 1/0 1/59
Router(config-line)# flush-at-activation
```

Related Commands

Command	Description
activation-character	Defines the character entered at a vacant terminal to begin a terminal session.
debug modem	Observes modem line activity on an access server.
modem dialin	Configures a line to enable a modem attached to the router to accept incoming calls only.
modem inout	Configures a line for both incoming and outgoing calls.
show line	Displays parameters of a terminal line.

ip alias

To assign an IP address to the service provided on a TCP port, use the **ip alias** command in interface configuration mode. To remove the specified address for the router, use the **no** form of this command.

ip alias *ip-address tcp-port*

no ip alias *ip-address*

Syntax Description

ip-address	Specifies the IP address for the service.
tcp-port	Specifies the number of the TCP port.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A user attempting to establish a connection is connected to the first free line in a rotary group using the Telnet protocol.

The IP address must be on the same network or subnet as the main address of the terminal server, and must not be used by another host on that network or subnet. Connecting to the IP address has the same effect as connecting to the main address of the router, using the argument *tcp-port* as the TCP port.

You can use the **ip alias** command to assign multiple IP addresses to the router. For example, in addition to the primary alias address, you can specify addresses that correspond to lines or rotary groups. Using the **ip alias** command in this way makes connection to a specific rotary group transparent to the user.

When asynchronous mode is implemented, the Cisco IOS software creates the appropriate IP aliases, which map the asynchronous addresses for the lines to which they are connected. This process is automatic and does not require configuration.

Examples

The following example configures connections to IP address 172.30.42.42 to act identically to connections made to the primary IP address of the server on TCP port 3001. In other words, a user is connected to the first free line on port 1 of the rotary group that uses the Telnet protocol.

```
ip alias 172.30.42.42 3001
```

ipx nasi-server enable

To enable NetWare Asynchronous Services Interface (NASI) clients to connect to asynchronous devices attached to your router, use the **ipx nasi-server enable** command in global configuration mode. To prevent NASI clients from connecting to asynchronous devices through a router, use the **no** form of this command.

ipx nasi-server enable

no ipx nasi-server enable

Syntax Description

This command has no arguments or keywords.

Command Default

NASI is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you enter this command, NASI clients can connect to any port on the router, other than the console port, to access network resources. When the user on the NASI client uses the Windows or DOS application to connect to the router, a list of available tty and vty lines appear, beginning with tty1. The user can select the desired outgoing tty or vty port.

To to enable a username and password prompt for authentication, authorization, and accounting purposes, you can configure TACACS+ security on the router, after the user on the NASI client selects a tty or vty port.

Examples

The following example shows a minimum configuration to enable NASI clients dial-in access with TACACS+ authentication:

```
ipx routing
ipx internal-network ncs001
interface ethernet 0
  ipx network 1
ipx nasi-server enable
! enable TACACS+ authentication for NASI clients using the list name swami
aaa authentication nasi swami tacacs+
line 1 8
  modem inout
```

Related Commands

Command	Description
aaa authentication nasi	Specifies AAA authentication for NASI clients connecting through the access server.
nasi authentication	Enables AAA authentication for NASI clients connecting to a router.
show ipx nasi connections	Displays the status of NASI connections.
show ipx spx-protocol	Displays the status of the Sequenced Packet Exchange (SPX) protocol stack and related counters.

keymap

To define specific characteristics of keyboard mappings, use the **keymap** command in global configuration mode. To remove the named keymap from the current image of the configuration file, use the **no** form of this command.

keymap *keymap-name keymap-entry*

no keymap *keymap-name*

Syntax Description

keymap-name	Name of the file containing the keyboard mappings. The name can be up to 32 characters long and must be unique.
keymap-entry	Commands that define the keymap.

Defaults

VT100 keyboard emulation

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **keymap** command maps individual keys on a non-TN3270 keyboard to perform the function defined for the TN3270 keyboard. Use the **show keymap** EXEC command to test for the availability of a keymap.

Do not use the name “default” for a ttycap entry filename or the Cisco IOS software will adopt the newly defined entry as the default.

The guidelines for creating a keymap follow.

The Keymap Entry Structure

A keymap is a keyboard map file. A keymap consists of an entry for a keyboard. The first part of a keymap lists the names of the keyboards that use that entry. These names will often be the same as in the ttycaps (terminal emulation) file, and often the terminals from various ttycap entries will use the same keymap entry. For example, both 925 and 925vb (for 925 with visual bells) terminals would probably use the same keymap entry. There are other circumstances in which it is necessary to specify a keyboard name as the name of the entry (for example, if a user requires a custom key layout).

After the names, which are separated by vertical bars (|), comes an open brace ({), the text that forms the definitions, the a close brace (}), as follows:

```
ciscodefault{
clear = '^z';\
flinp = '^x';\
    enter = '^m';\
    delete = '^d' | '^?';\
    synch = '^r';\
    ebcdic_xx='string'
    reshow = '^v';
    eeof = '^e';\
    tab = '^i';\
    btab = '^b';\
    nl = '^n';\
    left = '^h';\
    right = '^l';\
    up = '^k';\
    down = '^j';\
    einp = '^w';\
    reset = '^t';\
    ferase = '^u';\
    insrt = '\E ';\
    pa1 = '^p1'; pa2 = '^p2'; pa3 = '^p3';\
    pfk1 = '\E1'; pfk2 = '\E2'; pfk3 = '\E3'; pfk4 = '\E4';\
    pfk5 = '\E5'; pfk6 = '\E6'; pfk7 = '\E7'; pfk8 = '\E8';\
    pfk9 = '\E9'; pfk10 = '\E0'; pfk11 = '\E-'; pfk12 = '\E=';\
    pfk13 = '\E!'; pfk14 = '\E@'; pfk15 = '\E#'; pfk16 = '\E$';\
    pfk17 = '\E%'; pfk18 = '\E'; pfk19 = '\E&'; pfk20 = '\E*';\
    pfk21 = '\E('; pfk22 = '\E)'; pfk23 = '\E_'; pfk24 = '\E+';\
}
```

Each definition consists of a reserved keyword, which identifies the TN3270 function, followed by an equal sign (=), followed by the various ways to generate this particular function, followed by a semicolon (;), as follows:

```
pa1 = '^p1'; pa2 = '^p2'; pa3 = '^p3';\
```

Each alternative way to generate the function is a sequence of ASCII characters enclosed inside single quotes (`''`); the alternatives are separated by vertical bars (|), as follows:

```
delete = '^d' | '^?';\
```

Inside the single quotes, a few characters are special. A caret (^) specifies that the next character is a control (Ctrl) character. The two-character string caret-a (^a) represents Ctrl-a. The caret-A sequence (^A) generates the same code as caret-a (^a). To generate Delete (or DEL), enter the caret-question mark (^?) sequence.

Note The Ctrl-caret combination (Ctrl-^), used to generate a hexadecimal 1E, is represented as two caret symbols in sequence (^^)—not as a caret-backslash-caret combination (^\^).

In addition to the caret, a letter can be preceded by a backslash (\). Because this sequence has little effect for most characters, its use is usually not recommended. In the case of a single quote (`'`), the backslash prevents that single quote from terminating the string. In the case of a caret (^), the backslash prevents the caret from having its special meaning. To include the backslash in the string, place two backslashes (\\) in the keymap. Table 2 lists other supported special characters.

Table 2 Special Characters Supported by TN3270 Keymap Capability

Character	Description
\E	Escape character
\n	Newline

Table 2 Special Characters Supported by TN3270 Keymap Capability (continued)

Character	Description
\t	Tab
\r	Carriage return

Each character in a string needs not be enclosed within single quotes. For example, \E\E\E means three escape characters.

To enter a keymap, provide a unique name for it and explicitly define all special keys you intend to include in it within open and close braces. Also, except for the last line, each line must be terminated with a backslash symbol (\). The last line ends with the closing bracket (}) symbol and an end-of-line character.

Keymap Restrictions

When IBM-style TN3270 terminals are emulated, a mapping must be performed between sequences of keys pressed at an ASCII keyboard and the keys available on a TN3270 keyboard. For example, a TN3270 keyboard has a key labeled EEOF that erases the contents of the current field from the location of the cursor to the end. To accomplish this function, the terminal user and a program emulating a TN3270 keyboard must agree on which keys will be typed to invoke the function. The requirements for these sequences follow:

- The first character of the sequence must be outside of the standard ASCII printable characters.
- No sequence can be a complete subset of another sequence (although sequences can share partial elements).

Following are examples of acceptable keymap entries:

```
pfk1 = '\E1';
pfk2 = '\E2';
```

Following are examples of unacceptable keymap entries:

```
pfk1 = '\E1';
pfk11 = '\E11';
```

In the acceptable example, the keymap entry for pfk1 is not completely included in the keymap entry for pfk2. By contrast, in the unacceptable, or conflicting keymap pair, the sequence used to represent pfk1 is a complete subset of the sequence used to represent pfk11. See the keymap entry provided later in the Examples section of how various keys can be represented to avoid this kind of conflict.

Table 3 lists TN3270 key names that are supported in this keymap. Note that some of the keys do not exist on a TN3270 keyboard. An unsupported function will cause the Cisco IOS software to send a (possibly visual) bell sequence to the terminal.

Table 3 TN3270 Key Names Supported by Defaults Keymap

TN3270 Key Name	Functional Description
LPRT	Local print[1]
DP	Duplicate character
FM	Field mark character
CURSEL	Cursor select
CENTSIGN	EBCDIC cent sign

Table 3 TN3270 Key Names Supported by Defaults Keymap (continued)

TN3270 Key Name	Functional Description
RESHOW	Redisplay the screen
EINP	Erase input
EEOF	Erase end of field
DELETE	Delete character
INSRT	Toggle insert mode
TAB	Field tab
BTAB	Field back tab
COLTAB	Column tab
COLBAK	Column back tab
INDENT	Indent one tab stop
UNDENT	Undent one tab stop
NL	New line
HOME	Home the cursor
UP	Up cursor
DOWN	Down cursor
RIGHT	Right cursor
LEFT	Left cursor
SETTAB	Set a column tab
DELTAB	Delete a column tab
SETMRG	Set left margin
SETHOM	Set home position
CLRTAB	Clear all column tabs
APLON	Apl on[1]
APLOFF	Apl off[1]
APLEND[1]	Treat input as ASCII
PCON	Xon/xoff on[1]
PCOFF	Xon/xoff off[1]
DISC	Disconnect (suspend)[1]
INIT	New terminal type[1]
ALTK	Alternate keyboard dvorak[1]
FLINP	Flush input
ERASE	Erase last character
WERASE	Erase last word[1]
FERASE	Erase field
SYNCH	In synchronization with the user
RESET	Reset key–unlock keyboard

Table 3 TN3270 Key Names Supported by Defaults Keymap (continued)

TN3270 Key Name	Functional Description
MASTER_RESET	Reset, unlock, and redisplay
XOFF	Please hold output[1]
XON	Please give me output[1]
WORDTAB	Tab to beginning of next word[1]
WORDBACKTAB	Tab to beginning of current or last word[1]
WORDEND	Tab to end of current or next word[1]
FIELDEND	Tab to last nonblank of current or next unprotected (writable) field[1]
PA1	Program attention 1
PA2	Program attention 2
PA3	Program attention 3
CLEAR	Local clear of the TN3270 screen
TREQ	Test request
ENTER	Enter key
PFK1 to PFK30	Program function key 1 program function key 30
ATTN	Attention
SYSREQ	System request

[1] Not supported by the Cisco TN3270 implementation.

Table 4 lists the proper keys used to emulate each TN3270 function when default key mappings are used.

Table 4 Keys Used to Emulate Each TN3270 Function with Defaults Keymap

Key Types	IBM TN3270 Key	Defaults Keys
Cursor movement keys	New Line	Ctrl-n or Home
	Tab	Ctrl-i
	Back Tab	Ctrl-b
	Back Tab	Ctrl-b
	Cursor Left	Ctrl-h
	Cursor Right	Ctrl-l
	Cursor Up	Ctrl-k
	Cursor Down	Ctrl-j or LINE FEED
Edit control keys	Delete Char	Ctrl-d or RUB
	Erase EOF	Ctrl-e
	Erase Input	Ctrl-w
	Insert Mode	ESC-Space[1]
	End Insert	ESC-Space

Table 4 Keys Used to Emulate Each TN3270 Function with Defaults Keymap (continued)

Key Types	IBM TN3270 Key	Defaults Keys
Program function keys	PF1	ESC 1
	PF2	ESC 2
	...	...
	PF10	ESC 0
	PF11	ESC -
	PF12	ESC =
	PF13	ESC !
	PF14	ESC @
	...	...
	PF24	ESC +
Program attention keys	PA1	Ctrl-p 1
	PA2	Ctrl-p 2
	PA3	Ctrl-p 3
Local control keys	Reset After Error	Ctrl-r
	Purge Input Buffer	Ctrl-x
	Keyboard Unlock	Ctrl-t
	Redisplay Screen	Ctrl-v
Other keys	Enter	Return
	Clear	Ctrl-z
	Erase current field	Ctrl-u

[1] ESC refers to the Escape key.

Examples

The following example is the default entry used by the TN3270 emulation software when it is unable to locate a valid keymap in the active configuration image. Table 3 lists the key names supported by the default Cisco TN3270 keymap.

```
keymap ciscodefault{
    clear = '^z';\
    flinp = '^x';\
    enter = '^m';\
    delete = '^d' | '^?';\
    synch = '^r';\
    reshow = '^v';\
    ebcdic_xx='string'
    eeof = '^e';\
    tab = '^i';\
    btab = '^b';\
    nl = '^n';\
    left = '^h';\
    right = '^l';\
    up = '^k';\
    down = '^j';\
    einp = '^w';\
    reset = '^t';\
    ferase = '^u';\
    insrt = '\E ';\
    pa1 = '^p1'; pa2 = '^p2'; pa3 = '^p3';\
    pfk1 = '\E1'; pfk2 = '\E2'; pfk3 = '\E3'; pfk4 = '\E4';\
    pfk5 = '\E5'; pfk6 = '\E6'; pfk7 = '\E7'; pfk8 = '\E8';\
    pfk9 = '\E9'; pfk10 = '\E0'; pfk11 = '\E-'; pfk12 = '\E=';\
    pfk13 = '\E!'; pfk14 = '\E@'; pfk15 = '\E#'; pfk16 = '\E$';\
    pfk17 = '\E%'; pfk18 = '\E'; pfk19 = '\E&'; pfk20 = '\E*';\
    pfk21 = '\E('; pfk22 = '\E)'; pfk23 = '\E_'; pfk24 = '\E+';\
}
```

The following keymap statement maps the “|” character to send EBCDIC 0x6A:

```
keymap mykeys{
ebcdic_6f='|'
}
```

Related Commands

Command	Description
keymap-type	Specifies the keyboard map for a terminal connected to the line.
show keymap	Tests the availability of a keymap after a connection on a router takes place.
terminal-type	Specifies the type of terminal connected to a line.

keymap-type

To specify the keyboard map for a terminal connected to the line, use the **keymap-type** command in line configuration mode. To reset the keyboard type for the line to the default, use the **no** form of this command.

keymap-type *keymap-name*

no keymap-type

Syntax Description

keymap-name	Name of a keymap defined within the configuration file of the router. The TN3270 terminal-type negotiations use the specified keymap type when setting up a connection with the remote host.

Defaults

VT100

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command must follow the corresponding **keymap** global configuration entry in the configuration file. The TN3270 terminal-type negotiations use the specified keymap type when setting up a connection with the remote host.

Setting the keyboard to a different keymap requires that a keymap be defined with the Cisco IOS software configuration either by obtaining a configuration file over the network that includes the keymap definition or by defining the keyboard mapping using the **keymap** global configuration command.

Use the command **show keymap** EXEC command to test for the availability of a keymap.

Examples

The following example sets the keyboard mapping to a keymap named vt100map:

```
line 3
 keymap-type vt100map
```

Related Commands

Command	Description
keymap	Defines specific characteristics of keyboard mappings.

Command	Description
show keymap	Tests the availability of a keymap after a connection on a router takes place.
ttycap	Defines characteristics of a terminal emulation file.

lat

To connect to a local-area transport (LAT) host, use the **lat** command in EXEC mode.

lat *name* [**node** *nodename* | **port** *portname* | **/debug**]

Syntax Description

name	LAT-learned service name.
node *nodename*	(Optional) Specifies a connection to a particular LAT node that offers a service. If you do not include the node name option, the node with the highest rating offering the service is used. Use the **show lat nodes** EXEC command to display information about all known LAT nodes.
port *portname*	(Optional) Specifies a destination LAT port name. This keyword is ignored in most time-sharing systems, but is used by routers and network access servers offering *reverse LAT* services. Reverse LAT involves connecting to one router from another, so that the target router runs the host portion of the protocol. Enter the port name in the format of the remote system as the *portname* argument.
/debug	(Optional) Enables a switch to display parameter changes and other special messages.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

After entering the **lat** command, you can quit the connection by pressing Ctrl-C, or complete the connection by entering the password for a given service.

You can have several concurrent LAT sessions open and switch between them. To open a subsequent session, first enter the escape sequence (**Ctrl-Shift-6** then **x** [**Ctrl^x**] by default) to suspend the current session. Then open a new session.

To list the available LAT services, use the **show lat services** EXEC command.

You can temporarily define the list of services to which you or another user can connect. To do so, use the **terminal lat out-group** command to define the group code lists used for connections from specific lines.

To exit a session, simply log off the remote system. Then terminate an active LAT session by entering the **exit** command.

If your preferred transport is set to **lat**, you can use the **connect** command in place of the **lat** command. Refer to the chapter “Configuring Terminal Operating Characteristics for Dial-In Sessions” in the *Cisco IOS Terminal Services Configuration Guide* for more information about configuring a preferred transport type. When your preferred transport is set to **none** or to another protocol, you must use the **lat** command to connect to a LAT host.

Examples

The following sample command and output shows a LAT connection from the router named Router_A to host eng2:

```
Router_A> lat eng2
Trying ENG2...Open
         ENG2 - VAX/VMS V5.2
Username: User1
Password:
    Welcome to VAX/VMS version V5.2 on node ENG2
    Last interactive login on Friday,  1-APR-1994 19:46
```

The system informs you of its progress by displaying the messages “Trying <system>...” and then “Open.” If the connection attempt is not successful, you receive a failure message.

The following sample command establishes a LAT connection from the router named Router_B to a device named our-modems and specifies port 24, which is a special modem:

```
Router_B> lat our-modems port 24
```

The following sample command establishes a LAT connection from the router named Router_C to a device named our-modems and specifies a node named eng:

```
Router_C> lat our-modems node eng
```

The following sample command and output shows the LAT session debugging capability:

```
Router_D> lat Eng2 /debug
Trying ENG2...Open
        ENG2 - VAX/VMS V5.2
 Username: User1
 Password:
    Welcome to VAX/VMS version V5.2 on node ENG2
    Last interactive login on Tuesday, 5-APR-1994 19:02
[Set Flow out off, Flow in on, Format 8:none, Speed 9600/9600]
[Set Flow out off, Flow in on, Format 8:none, Speed 9600/9600]
$ set ter/speed=2400
[Set Flow out off, Flow in on, Format 8:none, Speed 2400/2400]
```

A variety of LAT events are reported, including all requests by the remote system to set local line parameters. The messages within brackets ([ ]) are the messages produced by the remote system setting line characteristics to operating system defaults.

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
ip alias	Assigns an IP address to the service provided on a TCP port.
show lat services	Displays information about learned LAT services in the Cisco IOS software.
terminal lat out-group	Temporarily defines the list of services to which you or another user can connect.

lat access-list

To specify access conditions to nodes on the local-area transport (LAT) network, use the **lat access-list** command in global configuration mode. To remove a specified access list number, use the **no** form of this command.

lat access-list *number* {**permit** | **deny**} *nodename*

no lat access-list *number*

Syntax Description

number	Specifies a number ranging from 1 to 199 assigned to the line using the **access-class** line configuration command.
permit	Allows any matching node name to access the line.
deny	Denies access to any matching node name.
nodename	Specifies the name of the LAT node, with or without regular expression pattern matching characters, with which to compare for access. The UNIX-style regular expression characters allow for pattern matching of characters and character strings in the node name.

Defaults

No access conditions are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Regular expressions are case sensitive. Because LAT node names are always in all uppercase letters, make sure you use only all uppercase regular expressions.

Table 5 and Table 6 list pattern and character matching symbols and their use. A more complete description of the pattern matching characters is found in the "Regular Expressions" appendix in the *Cisco IOS Terminal Services Configuration Guide*.

Table 5 Pattern Matching

Character	Description
\0	Replaces the entire original address.
\1..9	Replaces the strings that match the first through ninth parenthesized part of X.121 address.
*	Matches 0 or more sequences of the regular expressions.

Table 5 Pattern Matching

Character	Description
+	Matches 1 or more sequences of the regular expressions.
?	Matches the regular expression of the null string.

Table 6 Character Matching

Character	Description
^	Matches the null string at the beginning of the input string.
$	Matches the null string at the end of the input string.
\char	Matches *char*.
.	Matches any single character.

Examples

The following example permits all packets destined for any LAT node named WHEEL:

```
lat access-list 1 permit WHEEL
```

The following example denies all packets destined for any LAT node name beginning with the BLDG1- prefix:

```
lat access-list 2 deny ^BLDG1-
```

Related Commands

Command	Description
accept dialin	Defines access list restrictions on incoming and outgoing connections.

lat enabled

To enable local-area transport (LAT), use the **lat enabled** command in interface configuration mode. To disable LAT, use the **no** form of this command.

lat enabled

no lat enabled

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables LAT on Ethernet interface 0:

```
interface ethernet 0
 lat enabled
```

The following example disables LAT on Ethernet interface 0:

```
interface ethernet 0
 no lat enabled
```

lat group-list

To allow a name to be assigned to the group list, use the **lat group-list** command in global configuration mode. To remove the specified group list, use the **no** form of this command.

lat group-list *groupname* {*number* | *range* | **all**} [**enabled** | **disabled**]

no lat group-list *groupname* {*number* | *range* | **all**} [**enabled** | **disabled**]

Syntax Description

groupname	Specifies a group code name.
number	Specifies a group code number. You can enter both a group code name and group code numbers.
range	Specifies a hyphenated range of numbers.
all	Specifies the range from 0 to 255.
enabled	(Optional) Allows incremental changes to the list; that is, you can add a group code without retyping the entire command.
disabled	(Optional) Allows selective removal of a group code from the list.

Defaults

None. A group list is any combination of group names, numbers, or ranges. No group names are assigned to the list by default.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Specifying a name for a group list simplifies the task of entering individual group codes. In other words, a name makes it easier to refer to a long list of group code numbers. The group list must already exist. Use the **show lat groups** EXEC command to see a list of existing groups.

Examples

The following example creates the new group named stockroom and defines it to include the group numbers 71 and 99:

```
lat group-list stockroom 71 99
```

The following example adds group code 101 to the group named stockroom:

```
lat group-list stockroom 101 enabled
```

The following example deletes the group named Bldg-2:

```
no lat group-list Bldg-2
```

Related Commands

Command	Description
lat out-group	Defines a group list for the outgoing user-initiated connections for a line.
lat service-group	Specifies a group code mask to use when advertising all services for this node and to control incoming services.
show lat groups	Displays the groups that were defined in the Cisco IOS software.

lat host-buffers

To set the number of receive buffers that will be negotiated when the router is acting as a local-area transport (LAT) host, use the **lat host-buffers** command in global configuration mode. To return to the default of one receive buffer, use the **no** form of this command.

lat host-buffers *receive-buffers*

no lat host-buffers *receive-buffers*

Syntax Description

receive-buffers	Specifies the number of receive buffers that will be negotiated. Valid values range from 1 to 128.

Defaults

One receive buffer

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before LAT Version 5.2, LAT allowed only one outstanding message at a time on a virtual circuit. This restriction could limit the performance of large routers. For example, only one Ethernet packet of data could be in transit at a time. With LAT Version 5.2, nodes can indicate that they are willing to receive more than one message at a time. During virtual circuit startup, each side communicates to the other how many outstanding messages it is willing to accept.

Examples

The following example enables LAT and configures the LAT host to negotiate 100 receive buffers:

```
lat enabled
lat host-buffers 100
```

Related Commands

Command	Description
lat server-buffers	Sets the number of receive buffers that will be negotiated when the router is acting as a LAT server.

lat ka-timer

To set the rate of the keepalive timer, use the **lat ka-timer** command in global configuration mode. To restore the default, use the **no** form of this command.

lat ka-timer *seconds*

no lat ka-timer

Syntax Description

seconds	Timer rate, in seconds. Valid values for the timer rate range from 10 to 255 seconds.

Defaults

20 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The keepalive timer sets the rate that messages are sent in the absence of actual traffic between the router and the remote node. The server uses keepalive messages to detect when communication with a remote node is disrupted or when the remote node has crashed.

Examples

The following example sets the keepalive timer rate to 5 seconds:

```
lat ka-timer 5
```

lat node

To change the local-area transport (LAT) node name without changing the system host name, use the **lat node** command in global configuration mode.

lat node *node-name*

Syntax Description

node-name	Name of the LAT node.

Defaults

No default LAT node name

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command allows you to give the server a node name that is different from the host name. Use the **show entry** EXEC command to determine which LAT hosts have queue entries for printers on the servers. Use the **clear entry** EXEC command to delete entries from the queue.

Examples

The following example specifies the LAT node name as DEC2:

```
lat node DEC2
```

Related Commands

Command	Description
clear entry	Deletes an entry from the list of queued host-initiated connections.
hostname	Specifies or modifies the host name for the network server.
show entry	Displays the list of queued host-initiated connections to a router.

lat out-group

To define a group list for outgoing user-initiated connections on a line, use the **lat out-group** command in line configuration mode. To return to the default value, use the **lat out-group 0** command.

lat out-group {*group-name number* | *range* | **all**}

Syntax Description

group-name	Group code name.
number	Group code number. You can also enter both a group code name and group code numbers.
range	Hyphenated range of numbers.
all	Range from 0 to 255.

Defaults

The default group code number is 0.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can have values for one, two, or all three arguments. If the **all** keyword is specified, no arguments can be used. You can enter the *group-name*, *number*, and *range* values in any order.

Use the **show lat groups** EXEC command to display group numbers. If the host node and router do not share a common group number, the host services will not be displayed.

Examples

The following example defines the services for lines 1 through 7, 10 through 17, and 20 through 24. Access to systems on the first set of lines is limited to groups 12 and 18 through 23; the second set is limited to group 12; the third set is limited to group codes 12, 18 through 23, and 44. All other lines use the default of group 0.

```
line 1 7
 lat out-group 12 18-23
line 10 17
 lat out-group 12
line 20 24
 lat out-group 12 18-23 44
```

Related Commands

Command	Description
lat group-list	Allows a name to be assigned to the group list, which is any combination of group names, numbers, or ranges.
show lat groups	Displays the groups that were defined in the Cisco IOS software with the **lat group-list** command.

lat remote-modification

To enable remote local-area transport (LAT) modification of line characteristics (for example, baud rate), use the **lat remote-modification** command in line configuration mode. To disable remote LAT modification of line characteristics, use the **no** form of this command.

lat remote-modification

no lat remote-modification

Syntax Description

This command has no arguments or keywords.

Defaults

Remote modification is disabled.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Enabling the line for remote modification allows the remote LAT node to change line characteristics (for example, baud rate, parity, and so on).

Examples

The following example enables remote LAT modification on line 4:

```
line 4
 lat remote-modification
```

lat retransmit-limit

To set the number of times that local-area transport (LAT) resends a message before declaring the remote system unreachable, use the **lat retransmit-limit** command in global configuration mode. To restore the default retry value, use the **no** form of this command.

lat retransmit-limit *number*

no lat retransmit-limit

Syntax Description

number	Number of retries. Valid values range from 4 to 255 retries.

Defaults

8 retries

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Assigning larger values to the number of tries increases the robustness of the LAT service at the cost of longer delays when communications are disrupted. Because LAT generally resends messages once per second, the value is approximately the number of seconds that LAT connections will survive connection disruption.

If you bridge LAT, the retransmission limit should be set to at least 20 tries for LAT sessions to survive a worst-case spanning-tree reconfiguration, because the time for bridging spanning-tree reconfiguration to be completed can be up to 15 seconds.

Examples

The following example sets the retransmission limit to 30 tries, enough time to sustain the downtime incurred when the system must reconfigure a spanning-tree topology:

```
lat retransmit-limit 30
```

lat server-buffers

To set the number of receive buffers that will be negotiated when the router is acting as a local-area transport (LAT) server, use the **lat server-buffers** command in global configuration mode. To return to the default of one receive buffer, use the **no** form of this command.

lat server-buffers *receive-buffers*

no lat server-buffers *receive-buffers*

Syntax Description

receive-buffers	Specifies the number of receive buffers that will be negotiated. Valid values range from 1 to 128 receive buffers. The default value is 1 receive buffer.

Defaults

1 receive buffer

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before LAT Version 5.2, LAT allowed only one outstanding message on a virtual circuit at a time. This restriction could limit the performance of large routers because only one Ethernet packet of data could be in transit at a time. With LAT Version 5.2, nodes can indicate that they are willing to receive more than one message at a time. During virtual circuit startup, each side communicates to the other how many outstanding messages it is willing to accept.

Examples

The following example enables LAT and configures the server to negotiate 25 receive buffers:

```
lat enabled
lat server-buffers 25
```

Related Commands

Command	Description
lat host-buffers	Sets the number of receive buffers that will be negotiated when the router is acting as a LAT host.

lat service enabled

To enable inbound connections to the specified service and enable the advertisement of this service to routers on the network, use the **lat service enabled** command in global configuration mode. To delete the named service, use the **no** form of this command.

lat service *service-name* **enabled**

no lat service *service-name* **enabled**

Syntax Description

service-name	Name of the service.

Defaults

No services are enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In the simplest form, this command creates a service that gives connecting users access to a vty port on the server.

Use the **lat service enabled** command after commands that define a service so that users do not connect to a service before all the parameters are set.

Deleting a service does not disconnect existing connections.

Examples

The following example enables inbound connections to the service named WHEEL:

```
lat service WHEEL enabled
```

lat service-host

To statically define local-area transport (LAT) services, use the **lat service-host** command in interface configuration mode. To remove the statically defined LAT services, use the **no** form of this command.

lat service-host *node-name service-name MACaddress*

no lat service-host

Syntax Description

node-name	The remote node providing this service.
service-name	The name of the service.
MAC address	MAC address entered as three hexadecimal numbers of four digits separated by a period MAC address of the remote node.

Command Default

LAT services are not statically defined.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **show running-config** command to verify if the LAT services have been configured.

Examples

The following example shows how to statically define LAT services:

```
Router# configure terminal
Router(config)# interface FastEthernet0/0
Router(config-if)# lat service-host node1 service1 0000.fc08.12ab
```

Related Commands

Command	Description
show running-config	Displays the running configuration.

lat service ident

To set the local-area transport (LAT) service identification for a specified service, use the **lat service ident** command in global configuration mode. To remove the identification, use the **no** form of this command.

lat service *service-name* **ident** *identification*

no lat service *service-name* **ident**

Syntax Description

service-name	Name of the service.
identification	Descriptive name (text only) that identifies the service.

Defaults

No LAT service identification is set for specific services.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The identification is advertised to other servers on the network and is displayed along with the list of name services on the LAN.

Examples

The following example specifies the identification “Welcome to Gateway-A” on the service named host1:

```
lat service host1 ident Welcome to Gateway-A
```

lat service password

To set up a local-area transport (LAT) password for a service, use the **lat service password** command in global configuration mode. To remove the password, use the **no** form of this command.

lat service *service-name* **password** *password*

no lat service *service-name* **password**

Syntax Description

service-name	Name of the service.
password	Password used to gain access to the service.

Defaults

No default LAT service passwords

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The connecting user will be required to enter the password to complete the connection. The password is obtained through the LAT password mechanism.

Examples

The following example specifies a service named host1 and the password secret:

```
lat service host1 password secret
```

lat service rating

To set a static service rating for the specified service, use the **lat service rating** command in global configuration mode. To remove the service rating, use the **no** form of this command.

lat service *service-name* **rating** *static-rating*

no lat service *service-name* **rating**

Syntax Description

service-name	Name of the service.
static-rating	Static service rating. The rating must be in the range from 1 to 255.

Defaults

Dynamic rating

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is not entered, the Cisco IOS software calculates a dynamic rating based on the number of free ports that can handle connections to the service. Setting a static rating overrides this calculation and causes the specified value to be used.

Examples

The following example specifies a service rating of 84 on the service named WHEEL:

```
lat service WHEEL rating 84
```

lat service rotary

To associate a rotary group with a service, use the **lat service rotary** command in global configuration mode. To remove the association, use the **no** form of this command.

lat service *service-name* **rotary** *group-number*

no lat service *service-name* **rotary**

Syntax Description

service-name	Name of the service.
group-number	Rotary group number.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Establish rotary groups using the **rotary** line configuration command.

When an inbound connection is received for this service, the router establishes a reverse local-area transport (LAT) connection to a terminal in that rotary group.

If the rotary option is not set, the connection will be to a virtual terminal session on the router.

Examples

The following example creates a service named MODEM to establish a rotary group:

```
lat services MODEM rotary 1
```

Related Commands

Command	Description
rotary	Defines a group of lines consisting of one of more lines.

lat service-announcements

To reenable local-area transport (LAT) broadcast service announcements, use the **lat service-announcements** command in global configuration mode. To disable the sending of LAT service announcements, use the **no** form of this command.

lat service-announcements

no lat service-announcements

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is enabled, the LAT code will periodically broadcast service advertisements. If the command is disabled, the LAT code will not send service announcements, so solicit information messages must be used to look up node information.

Note You should only disable service announcements if all of the nodes on the LAN support the service responder feature.

Examples

The following example reenables the sending of broadcast service announcements:

```
lat service-announcements
```

Related Commands

Command	Description
lat service-responder	Configures a node to act as proxy for other nodes when a solicit-information multicast message is received.

lat service-group

To specify a group code mask to use when advertising all services for this node and to control incoming services, use the **lat service-group** command in global configuration mode. To remove the group code mask specified, use the **no** form of this command.

lat service-group {[*groupname*] [*number*] [*min*-*max*] | **all**} [**enabled** | **disabled**]

no lat service-group {[*groupname*] [*number*] [*min*-*max*] | **all**} [**enabled** | **disabled**]

Syntax Description

groupname	Specifies a group code name. Multiple group code names can be specified.
number	Specifies a group code number. Multiple group code numbers can be specified. Valid values for the *number* argument range from 0 to 255.
min-*max*	Specifies a hyphenated range of numbers. Multiple group code number ranges can be specified. Valid values for the *min* and *max* arguments range from 0 to 255.
all	Specifies the group number range from 0 to 255.
enabled	(Optional) Allows incremental changes to the list; you can add a group code without retyping the entire command.
disabled	(Optional) Allows selective removal of a group code from the list.

Defaults

If no service group is specified, the Cisco IOS software defaults to advertising to group 0.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When this command is written to NVRAM (using the **write memory** EXEC command), the system looks for an exact match on a group code name. If it finds one, it uses that name in the command. Otherwise, it writes out a list of numbers, using the range syntax whenever possible.

Examples

The following example specifies groups 100 through 103, then defines engineering as the group code list to advertise:

```
lat group-list engineering 100-103
lat service-group engineering enabled
```

The following example specifies the groups 1, 5, 20 through 36, and 52:

```
lat service-group 1 5 20-36 52
```

Related Commands

Command	Description
lat group-list	Allows a name to be assigned to the group list, which is any combination of group names, numbers, or ranges.

lat service-responder

To configure a node to act as proxy for other nodes when a solicit-information multicast message is received, use the **lat service-responder** command in global configuration mode. To remove any proxy definition set up using the **lat service-responder** command, use the **no** form of this command.

lat service-responder

no lat service-responder

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Cisco IOS software can be configured to support the service responder feature that is part of the latest LAT Version 5.2 specification.

Specifically, the DECserver90L+, which has less memory than other Digital Equipment Corporation servers, does not maintain a cache of learned services. Instead, the DECserver90L+ solicits information about services as they are needed.

LAT Version 5.2 nodes can respond for themselves; however LAT Version 5.1 nodes, for example, VMS Version 5.4 or earlier nodes, cannot respond for themselves. Instead, a LAT Version 5.2 node configured as a service responder must respond in proxy for the LAT Version 5.1 nodes.

The Cisco IOS software can be configured as a LAT service responder. If all your nodes are LAT Version 5.2 nodes, you need not enable the service responder features.

Examples

The following example configures a node to act as a proxy for a node when a solicit-information multicast message is received. The node configured with this command will respond to solicit messages.

```
lat service-responder
```

Related Commands

Command	Description
lat service-announcements	Reenables LAT broadcast service announcements.

lat service-timer

To adjust the time between local-area transport (LAT) service advertisements, use the **lat service-timer** command in global configuration mode. To return to the default setting, use the **no** form of this command.

lat service-timer *seconds*

no lat service-timer

Syntax Description

seconds	Number of seconds between service announcements. Note that the granularity offered by this command is 10-second intervals, and the *seconds* value is rounded up.

Defaults

20 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command adjusts the time, in seconds, between LAT service announcements for services offered by the router. This function is useful in large networks with many LAT services and limited bandwidth.

Examples

The following example sets the interval between LAT service advertisements to 11, and it illustrates the rough granularity of the **lat service-timer** command:

```
! The time between LAT service advertisements is set to 11. Because the
! granularity is in ten-second intervals, the actual time between advertisement
! is 20 seconds.
lat service-timer 11
! 20 seconds between updates.
lat service-timer 19
! 120 seconds between updates.
lat service-timer 120
```

lat vc-sessions

To set the maximum number of sessions to be multiplexed onto a single local-area transport (LAT) virtual circuit, use the **lat vc-sessions** command in global configuration mode. To remove the definition of a prior session, use the **no** form of this command.

lat vc-sessions *maximum-number*

no lat vc-sessions *maximum-number*

Syntax Description

maximum-number	Specifies the number of sessions that will be multiplexed onto a single LAT virtual circuit. This number cannot be greater than 255.

Defaults

255 sessions per virtual circuit

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Setting the number of sessions to a lower number can increase throughput if many sessions are running on one host, especially with routers with many physical ports. It can also increase overhead if the same host has little traffic but a large number of sessions.

Examples

The following example sets the maximum number of sessions to be multiplexed onto a single LAT virtual circuit at 100:

```
lat vc-sessions 100
```

lat vc-timer

To set the interval of time local-area transport (LAT) waits before sending any traffic, use the **lat vc-timer** command in global configuration mode. To remove a timer definition, use the **no** form of this command.

lat vc-timer *milliseconds*

no lat vc-timer *milliseconds*

Syntax Description

milliseconds	Specifies the amount of time LAT will wait before sending traffic. Acceptable values range from 10 to 1000 milliseconds.

Defaults

80 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Smaller timer values increase the overhead on both the router and the host. However, you can use smaller values to correct buffer overflows, which happen when the router receives more data than it can buffer during a virtual circuit timer interval.

Larger values increase the need for buffering and can cause noticeable echoing delay. However, increased values can reduce traffic. In environments with slow bridging, retransmissions can be reduced if you increase the value to at least three times the worst-case, round-trip interval.

Examples

The following example sets the time between sending messages to 500 milliseconds:

```
lat vc-timer 500
```

line

To identify a specific line for configuration and enter line configuration collection mode, use the **line** command in global configuration mode.

line [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]

Syntax Description

aux	(Optional) Auxiliary EIA/TIA-232 DTE port. Must be addressed as relative line 0. The auxiliary port can be used for modem support and asynchronous connections.
console	(Optional) Console terminal line. The console port is DCE.
tty	(Optional) Standard asynchronous line.
vty	(Optional) Virtual terminal line for remote console access.
line-number	Relative number of the terminal line (or the first line in a contiguous group) that you want to configure when the line type is specified. Numbering begins with zero.
ending-line-number	(Optional) Relative number of the last line in a contiguous group that you want to configure. If you omit any keyword, then *line-number* and *ending-line-number* are absolute rather than relative line numbers.

Defaults

There is no default line.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can address a single line or a consecutive range of lines with the **line** command. A line number is necessary, though, and you will receive an error message if you forget to include it.

Entering the **line** command with the optional line type (**aux**, **console**, **tty**, or **vty**) designates the line number as a relative line number. For example, to configure line parameters for line 7 (a TTY line), you could enter the following:

```
line tty 7
```

You also can use the **line** command without specifying a line type. In this case, the line number is treated as an absolute line number. For example, to configure line parameters for line 5, which can be of any type, you could enter the following:

```
line 5
```

Absolute line numbers increment consecutively and can be difficult to manage on large systems. Relative line numbers are a shorthand notation used in configuration. Internally, the Cisco IOS software uses absolute line numbers. You cannot use relative line numbers everywhere, but you can use absolute line numbers everywhere.

The absolute line number of the auxiliary port is 1. The relative line number of the auxiliary port is 0. See the **modem** line configuration command to set up modem support on the auxiliary port.

The software keeps a table of absolute and relative line numbers that you can display with the **show users all** EXEC command. A sample display follows:

```
Router> show users all

  Line      User      Host(s)               Idle   Location
   0 con 0                                          con2 console
   1 tty 1                                          Engineering printer
   2 tty 2
   3 tty 3           HOST1                1:07   Employee1 x1111
   4 tty 4                                          Console E3-D
   5 tty 5                                          Mkt. demo area
   6 tty 6
   7 tty 7           HOST1                  14   Employee2 x1112
  10 tty 10
.
.
.
 135 tty 135
 136 tty 136
 137 tty 137                                      rp4-printer
 140 tty 140                                      Braille printer
 141 aux 0
 142 vty 0   User1     idle                       ROUTER-MAC.CISCO.COM
 143 vty 1   User2     idle                     0 HOST1.CISCO.COM
 144 vty 2
 145 vty 3
 146 vty 4
 147 vty 5
```

The absolute line numbers are listed at the far left, followed by the line type, and then the relative line number. Relative line numbers always begin numbering at zero and define the type of line. Addressing the second virtual terminal line as line VTY 1, for example, is easier than remembering it as line 143—its absolute line number.

The line types are ranked as follows in the line table:

1. Console 0 (con 0)
2. Standard asynchronous line (TTY)
3. Auxiliary port (aux)
4. Virtual terminal line (VTY)
5. Printer

The terminal from which you locally configure the router is attached to the console port. To configure line parameters for the console port, enter the following:

```
line console 0
```

The console relative line number must be 0.

Virtual terminal lines are used to allow remote access to the router. A virtual terminal line is not associated with either the auxiliary or console port. The router has five virtual terminal lines by default. However, you can create additional virtual terminal lines as described in the chapter "Configuring Protocol Translation and Virtual Asynchronous Devices" in the *Cisco IOS Terminal Services Configuration Guide*.

Configuring the console port or virtual terminal lines allows you to perform such tasks as setting communication parameters, specifying autobaud connections, and configuring terminal operating parameters for the terminal you are using.

Examples

The following example starts configuration for virtual terminal lines 0 to 4:

```
line vty 0 4
```

In the following example, the user creates and configures the maximum 100 virtual terminal lines with the **no login** command:

```
line vty 0 99
 no login
```

In the following example, the user eliminates virtual terminal line number 5 and all higher-numbered virtual terminal lines. Only virtual terminal lines 0 to 4 will remain.

```
no line vty 5
```

In the following example, the user configures console line 0, auxiliary line 0, and virtual terminal lines 0 to 4:

```
line vty 0 4
 login
line console 0
 password secretWord
line aux 0
 password Mypassword
 no exec
 access-class 1 in
 speed 19200
line vty 0
 exec-timeout 0 0
 password Mypassword
line vty 1
 exec-timeout 0 0
 password Mypassword
line vty 2
 exec-timeout 0 0
 password Mypassword
line vty 3
 password Mypassword
line vty 4
 password Mypassword
```

Related Commands

Command	Description
show line	Displays the parameters of a terminal line.
show users	Displays information about the active lines on the router.

login (EXEC)

To change a login username, use the **login** command in EXEC mode.

login

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can change a login username if you must match outgoing access list requirements or other login prompt requirements.

When you enter this command, the Cisco IOS software prompts you for a username and password. Enter the new username and the original password. If the username does not match, but the password does, the Cisco IOS software updates the session to the new username with which the **login** command attempt was made.

If no username and password prompts appear when you enter this command, the network administrator did not specify that a username and password be required at login time. If both the username and password are entered correctly, the session becomes associated with the specified username.

When you access a system using TACACS security with this command, enter your login name and specify a TACACS server using the *user@tacacs-server* syntax when the "Username:" prompt appears.

The TACACS server must be one of those defined in a Cisco IOS software configuration file. For more information, refer to the sections about specifying a TACACS host in the *Cisco IOS Security Configuration Guide*, or refer to the **tacacs-server host** command in the *Cisco IOS Security Command Reference*.

If you do not specify a host, the Cisco IOS software tries each of the TACACS servers in the list until it receives a response.

If you do specify a host that does not respond, no other TACACS server is queried. The Cisco IOS software will deny access or function according to the action specified by the **tacacs-server last-resort** command, if one is configured.

If you specified a TACACS server host with the *user@tacacs-server* command, the TACACS server specified will be used for all subsequent authentication or notification queries, with the possible exception of Serial Line Internet Protocol (SLIP) address queries.

Examples

The following example shows how login usernames and passwords can be changed. In this example, a user currently logged in under the username user1 attempts to change that login name to user2. After entering the **login** command, the user enters the new username, but enters an incorrect password. Because the password does not match the original password, the system rejects the attempt to change the username.

```
Router> login
Username: user2
Password:
% Access denied
Still logged in as "user1"
```

Next, the user attempts the login change again, with the username user2, but enters the correct (original) password. This time the password matches the current login information, the login username is changed to user2, and the user is allowed access to the EXEC at the user level.

```
Router> login
Username: user2
Password:
Router>
```

Related Commands

Command	Description
line-power	Sets up a temporary password on a line.
lockable	Enables the **lock** EXEC command.
password	Specifies a password on a line.
tacacs-server host	Specifies a TACACS+ host.

login (line)

To enable password checking at login, use the **login** command in line configuration mode. To disable password checking and allow connections without a password, use the **no** form of this command.

login [**local** | **tacacs**]

no login

Syntax Description

local	(Optional) Selects local password checking. Authentication is based on the username specified with the **username** global configuration command.
tacacs	(Optional) Selects the TACACS-style user ID and password-checking mechanism.

Defaults

Virtual terminals require a password. If you do not set a password for a virtual terminal, it responds to attempted connections by displaying an error message and closing the connection.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you specify the **login** command without the **local** or **tacacs** option, authentication is based on the password specified with the **password** line configuration command.

Note This command cannot be used with AAA/TACACS+. Cisco recommends that you use the **login authentication** command instead of the **login** (line) configuration command. Refer to the *Cisco IOS Security Command Reference* for a description of the **login authentication** command.

Examples

The following example sets the password letmein on vty 4:

```
line vty 4
 password letmein
 login
```

The following example enables the TACACS-style user ID and password-checking mechanism:

```
line 0
 password mypassword
 login tacacs
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
virtual-profile aaa	Enables virtual profiles by AAA configuration.

login-string

To define a string of characters that is sent to a host after a successful Telnet connection, use the **login-string** command in global configuration mode. To remove the login string, use the **no** form of this command.

login-string *host-name d message* [%*sec***p**] [%*sec***w**] [%**b**] [%**m**] *d*

no login-string *host-name*

Syntax Description

host-name	Specifies the name of the host.
d	Sets a delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the busy message.
message	Specifies the login string.
%*sec***p**	(Optional) Sets a pause in seconds. To insert pauses into the login string, embed a percent sign (%) followed by the number of seconds to pause and the letter "p."
%*sec***w**	(Optional) Prevents users from issuing commands or keystrokes during a pause.
%**b**	(Optional) Sends a Break character.
%**m**	(Optional) Supports TN3270 terminals. Sends only CR and no LINE FEED.

Defaults

No login strings are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character. To use a percent sign in the login string, precede it with another percent sign; that is, type the characters "%%." The options can be used anywhere within the message string.

This command applies only to rlogin and Telnet sessions.

Examples

In the following example, the value *%5p* causes a 5-second pause:

```
login-string office #ATDT 555-0134
%5p hello
#
```

match (ruleset)

To identify a connection for processing by a protocol translation ruleset, use the **match** command in translate ruleset configuration mode. To remove the match statement, use one of the two **no** forms of this command.

match [#*line-number*] *incoming-connection-parameter regular-expression* [#*line-number incoming-connection-parameter regular-expression* [...]]

no match *incoming-connection-parameter regular-expression* [*incoming-connection-parameter regular-expression* [...]]

no match #*line-number* [...]

Syntax Description

#*line-number*	(Optional) The line in the ruleset to test for a match operation. The # character must be entered.
incoming-connection-parameter	An incoming protocol parameter to test for; parameters are available for packet assembler/disassembler (PAD) and Telnet connections and are listed in Table 7 and Table 8.
regular-expression	Regular expression pattern to match.
[...]	(Optional) Specifies that multiple entries can be made as follows: • Up to six **match** tests can be written on one command line. • Multiple line numbers can be specified using the second **no** form of this command.

Defaults

No default behavior or values

Command Modes

Translate ruleset configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Up to six match tests can be written on one command line. The ellipses in the format shown above means multiple match test statements can be specified.

The **match** command is specific to the identified ruleset. A connection can be identified for processing by the ruleset match operation where tests written using keywords from Table 7 and Table 8, such as **dest-addr** and **dest-port**, match a regular expression.

Each protocol translation ruleset must have at least one match statement. If an incoming connection does not match any tests written in this template, it is not selected for processing by the ruleset.

The ordered set of commands in the template have line numbers that can be displayed using the **show translate** EXEC command.

Cisco regular expressions are described in Appendix A, "Regular Expressions," in the *Cisco IOS Terminal Services Configuration Guide*.

Table 7 and Table 8 lists the protocol parameter keywords that can be specified in the match test statements for incoming PAD and Telnet connections.

Table 7 Match Keywords for Incoming PAD Connections

Keyword	Description
cud *ASCII-string*	Call user data (CUD) that occurs after the protocol identification (PID). For outgoing PAD connections, this is the optional, user-specified text included in the outgoing call request packet following the protocol identification bytes. The CUD is entered as an ASCII string.
dest-addr *address*	Destination X.121 address entered as a number from 0 to 15 digits long.
dest-addr-ext *address*	Network service access point (NSAP) destination address extension.
dlci *number*	Frame Relay data-link connection identifier (DLCI) of an Annex G service entered as a number from one to seven digits in length, although a size of two to four digits is more likely, or the NULL string if not received on an Annex G service.
interface *type number*	Interface to be used for the circuit, entered using standard Cisco IOS interface designations: Serial1/0:1, for example.
mac *address*	Connection-Mode Network Service (CMNS) service remote host MAC address entered as three hexadecimal numbers of four digits separated by a period (0000.fc08.12ab, for example) or the NULL string if not received on a CMNS service.
packetsize *size*	X.25 maximum data packet sizes to request, entered as two numbers from the following choices: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096.
pid *byte-string*	Protocol identification (PID) string specified in ASCII or hexadecimal. A hexadecimal PID must be prefixed by "0x." For example, 0x01000000 is the standard PAD PID. Although it is available for specifying a nonstandard Call PID, this parameter is not restricted to the common PID length and can be used to specify the entire user data field.
reversed *flag*	Flag to indicate whether a reverse charged Call is permitted. This flag applies to a switched virtual circuit (SVC) and is entered as a single character, **Y** or **N**, for yes or no.
source-addr *address*	Source X.121 address.
source-addr-ext *address*	NSAP source address extension.
windowsize *size*	X.25 window sizes to request, entered as two numbers in a range from 1 to 127.
xot-dest-addr *address*	Destination IP address of an X.25 over TCP (XOT) service entered in standard IP address dotted decimal notation (10.0.0.127, for example) or the NULL string if not received on an XOT service.
xot-source-addr *address*	Source IP address of an XOT service entered in standard IP address dotted decimal notation (10.0.0.127, for example) or the NULL string if not received on an XOT service.

Table 8 Match Keywords for Incoming Telnet Connections

Keyword	Description
dest-addr *address*	Destination IP address entered in standard IP address dotted decimal notation: 10.0.0.127, for example.
dest-port *port*	Destination port entered as a decimal number from one to five digits long.
source-addr *address*	Source IP address entered in standard IP address dotted decimal notation: 10.0.0.127, for example.

Examples

The following example shows how to write match and skip tests to ignore connection attempts from any subnetwork address starting with 10 and match only those with a specific IP address and destination port number:

```
translate ruleset customer-case-1 from telnet to pad
 ! Ignore an incoming Telnet attempt from any subnetwork address starting with 10
 skip source-addr ^10\.*
 ! Match an incoming Telnet attempt destined for an IP addresses starting
 ! with 172.18., and a 5-digit port starting with 10 or 11
 match dest-addr ^172\.18\..* dest-port ^1[0-1]...$
 ! Or match an incoming Telnet attempt destined an IP addresses starting
 ! with 172.18., and a 5-digit port starting with 120 through 127
 match dest-addr ^172\.18\..* dest-port ^12[0-7]..$
```

The following example shows how to write match and skip tests to skip connection attempts from destination 55554 and to match only those with destination addresses from 55550 to 55553 and from 55556 to 55559:

```
translate ruleset A from pad to telnet
 skip dest-addr ^55554$
 match dest-addr ^5555.$
```

Related Commands

Command	Description
description (ruleset)	Adds a description about a translation ruleset.
options (ruleset)	Specifies protocol translation options in a translation ruleset.
set (ruleset)	Unconditionally sets one or more connection parameters to a fixed value for a translation ruleset.
show translate ruleset	Displays a summary of a specific or of all configured translation rulesets, behavioral parameters, and usage statistic.
skip (ruleset)	Identifies a connection for omission by the translation ruleset.
substitute (ruleset)	Matches an available protocol and substitutes another in a translation ruleset.
test (ruleset)	Tests parameter values in a translation ruleset using regular expressions.
test translate	Displays a trace of protocol translation behavior for a connection attempt.
translate ruleset	Defines a unique name for a translation ruleset, specifies translated protocols, and enters translate ruleset configuration mode.
x25 pvc translate ruleset	Configures PVCs that are valid for protocol translation rule set handling.

monitor traffic line

To monitor inbound or outbound asynchronous character mode traffic on another terminal line, use the **monitor traffic line** command in privileged EXEC mode.

monitor traffic line [**aux** | **tty**] *line-number* [**in** | **out**] [**control-char**] [**interactive**]

Syntax Description

aux	(Optional) Auxiliary EIA/TIA-232 DTE port. Must be addressed as relative line 0. The auxiliary port can be used for modem support and asynchronous connections.
tty	(Optional) Standard asynchronous line.
line-number	Relative number of the terminal line that you want to monitor when the line type is specified. Numbering begins with zero. Absolute number of the terminal line that you want to monitor when the line type is not specified. The acceptable range of this value is platform dependent.
in	(Optional) Inbound traffic is monitored.
out	(Optional) Outbound traffic is monitored.
control-char	(Optional) Control characters are displayed along with asynchronous character mode traffic. Control character display is turned off by default.
interactive	(Optional) Commands entered on the remote monitoring station are displayed to the user of the terminal line being monitored. By default, commands entered at the remote monitoring station are not displayed on the station being monitored (the keyboard lock is on).

Defaults

Outbound traffic is monitored.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.3(8)T	The **control-char** and **interactive** keywords were introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **monitor traffic line** command allows for the monitoring of only tty and auxiliary lines. The monitoring of console or vty lines is not permitted.

You can monitor only a single line with the **monitor traffic line** command. A line number is necessary, though, and you will receive an error message if you forget to include it.

To disable asynchronous line monitoring, enter the escape sequence (Ctrl-Shift-6, then x [Ctrl^x] by default).

Entering the **monitor traffic line** command with the optional line type (**aux** or **tty**) designates the line number as a relative number. For example, to configure line monitoring for line 7 (a tty line), you could enter the following:

```
monitor traffic line tty 7
```

You can also use the **monitor traffic line** command without specifying a line type. In this case, the line number is treated as an absolute line number. For example, to configure line traffic monitoring for line 5, which can be of **aux** or **tty** type, you could enter the following:

```
monitor traffic line 5
```

The **monitor traffic line** command starts displaying the asynchronous characters traversing the line that is being monitored. To stop monitoring traffic, enter the escape sequence (Ctrl-Shift-6, then x [Ctrl^x] by default).

You can issue the **control-char** keyword with the **monitor traffic line** command to configure the display of control characters along with the asynchronous character traffic on the line that is being monitored.

Note The **monitor traffic line** command inserts a linefeed (LF) character in the character stream immediately after a carriage return (CR) character if the CR character is not immediately followed by an LF character in the original character stream.

In releases prior to Cisco IOS Release 12.3(8)T, when the **monitor traffic line** command is running and the asynchronous characters are being displayed (the user has not yet entered the escape sequence to stop traffic monitoring), the Asynchronous Line Monitoring feature allows the user of the remote monitoring station to enter more commands on this line. The output of the additional commands are displayed not only to the user of the remote monitoring station but also to the user of the terminal line that is being monitored. To prevent this display of command output on the terminal line that is being monitored, the user of the remote monitoring station must be careful not to enter more commands while the **monitor traffic line** command is still running.

In Release 12.3(8)T, the default behavior of the **monitor traffic line** command was changed so that commands entered by the user on the remote monitoring station are not displayed to the user on the terminal line being monitored (the keyboard lock is on). The **interactive** keyword turns off the keyboard lock, enabling the display of commands entered on the remote monitoring station to the user of the terminal line being monitored.

Examples

The following example allows the user to monitor inbound asynchronous character mode traffic on tty line 10:

```
Router# monitor traffic line tty 10 in
```

The following example allows the user to monitor inbound asynchronous character mode traffic, including control characters, on tty line 10:

```
Router# monitor traffic line tty 10 in control-char
```

The following example allows the user to monitor inbound asynchronous character mode traffic on line 5. The **interactive** keyword turns off the keyboard lock, specifying that commands entered at the remote monitoring station will be displayed to the user of the line being monitored.

```
Router# monitor traffic line 5 in interactive
```

options (ruleset)

To specify protocol translation options in a translation ruleset, use the **options** command in translate ruleset configuration mode. To remove or change the option, use the **no** form of this command.

options *rule-option* [*rule-option* […]]

no options […]

Syntax Description

rule-option […]	One of the protocol translation option keywords listed in Table 9 followed, for some keywords, by a value for the option. More than one option can be listed on a command line.

Defaults

No default behavior or values

Command Modes

Translate ruleset configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to set the supported options listed in Table 9. The ellipses in the format shown above means multiple options statements can be specified. The ruleset-defined options are overwritten each time the **options** command is entered. A connection that matches a ruleset, but fails the ruleset's configured option test, will be rejected.

Table 9 Options for Translation Rulesets

Options Keyword	Description
access-class *number*	Access class number that the incoming source hosts must match, and that must already have been defined in an access list. Standard access list numbers are in the range from 1 to 99; expanded standard access lists numbers are in the range from 1300 to 1999.
login	Require a login on the incoming connection before the outgoing connection is attempted. No value is required for this keyword.
max-users *number*	Defines the maximum number of concurrent users allowed per ruleset. When the maximum user limit has been reached, subsequent connection attempts and a test with **test translate** command will be refused.
quiet	Suppress translation information messages on the session. No value is required for this keyword.

Examples

The following example limits the number of simultaneous ruleset users to 10 and requires that the user log in before the outgoing connection is made:

```
translate ruleset customer-case-1 from telnet to pad
 ! Match an incoming Telnet attempt destined for IP addresses starting
 ! with 172.18., and a 5-digit port starting with 120 through 127
 match dest-addr ^172\.18\..* dest-port ^12[0-7]..$
 ! Once the correct network is matched, specify that this ruleset is limited
 ! to ten concurrent users and requires a login exchange
 options max-users 10 login
```

Related Commands

Command	Description
description (ruleset)	Adds a description about a translation ruleset.
match (ruleset)	Identifies a connection for processing by the translation ruleset.
set (ruleset)	Unconditionally sets one or more connection parameters to a fixed value for a translation ruleset.
show translate ruleset	Displays a summary of a specific or of all configured translation rulesets, behavioral parameters, and usage statistic.
skip (ruleset)	Identifies a connection for omission by the translation ruleset.
substitute (ruleset)	Matches an available protocol and substitutes another in a translation ruleset.
test (ruleset)	Tests parameter values in a translation ruleset using regular expressions.
test translate	Displays a trace of protocol translation behavior for a connection attempt.
translate ruleset	Defines a unique name for a translation ruleset, specifies translated protocols, and enters translate ruleset configuration mode.
x25 pvc translate ruleset	Configures PVCs that are valid for protocol translation rule set handling.

pad

To log in to a packet assembler/disassembler (PAD), use the **pad** command in EXEC mode.

pad {*x121-address* | *host-name*} [**/cud** *text*] [**/debug**] [**/profile** *name*] [**/quiet** *message*] [**/reverse**] [**/use-map**]

Syntax Description

x121-address	Specifies the X.121 address of the X.25 host.
host-name	Specifies the X.25 host name if the host-to-address mapping has been set with the **X.25 host** command.
/cud *text*	(Optional) Includes the specified *text* in the Call User Data (CUD) field of the outgoing Call Request Packet. The **/** character is required.
/debug	(Optional) Displays the informational level of logging messages whenever the remote host changes an X.3 parameter setting or sends any other X.29 control packet. The **/** character is required.
/profile *name*	(Optional) Sets X.3 PAD parameters for the *name* script. Using this keyword and profile name argument is the same as issuing the **x29 profile** global configuration command when translating X.25. If the X.29 profile is set to **default**, the profile is applied to all incoming X.25 PAD calls, including the calls used for protocol translation. The **/** character is required.
/quiet *message*	(Optional) Suppresses information messages. Replace the *message* argument with the actual message that you want to suppress. The **/** character is required.
/reverse	(Optional) Causes reverse-charge calls to be accepted on a per-call (rather than a per-interface) basis. The **/** character is required.
/use-map	(Optional) Applies **x25 map pad** command entry options (such as CUD and idle) and facilities (such as packet in, packet out, win in, and win out) to the outgoing PAD call. This function occurs only if a matching X.121 destination address exists in an **x25 map pad** command entry. The **/** character is required.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **pad** command supports one-word connections. You need not enter the **pad** command; entering the address is enough to start the connection. A PAD can also be accessed and X.3 parameters configured with the **x28** EXEC command, which uses the standard X.28 user interface.

You can have several PAD connections open at the same time and switch between them. You also can exit a connection and return to the user EXEC prompt at any point. To open a new connection, first exit the current connection by entering the escape sequence (**Ctrl-Shift-6** then **x** [**Ctrl^x**] by default) to return to the EXEC prompt, then open the new connection. If the **/use-map** option is selected on the outgoing **pad** command, the **x25 map pad** command entries are searched for a matching X.121 destination address. If a match is found, the **x25 map pad** command entry options (such as CUD and idle) and facilities (such as packet in, packet out, win in, and win out) are applied to the outgoing PAD call.

To display information about packet transmission and X.3 PAD parameter settings, use the **show x25 pad** command. To exit a session, simply log out of the remote system. Then, terminate the active session by entering the **exit** command.

Examples

Use the **?** command to display **pad** command options, as shown in the following example:

```
Router# pad / ?
  /cud      Call user data
  /debug    Debugging option
  /profile  Use a defined X.3 profile
  /quiet    Suppress informational messages
  /reverse  X25 Address reverse
  /use-map  Use x25 map pad command facilities for outgoing Calls
```

The following example starts a PAD session:

```
Router> pad 123456789
Trying 123456789...Open
Router>
```

You can also access a PAD using standard X.28 commands. The following example enters X.28 mode with the **x28** EXEC command and configures a PAD with the **set** X.3 parameter command. The **set** command sets the idle time delay to 40 seconds.

```
Router# x28
* set 4:40
```

The following example uses the **/use-map** option to configure a larger window and packet size than the default specified on the interface, and it sets the virtual circuit idle time to 2 seconds. Notice that the map values are used rather than the interface default values.

```
Router-A(config-if)# x25 map pad 2194441 cud user1 windowsize 7 7 packetsize 1024 1024
idle 2
Router-A(config-if)# end
Router-A#
%SYS-5-CONFIG_I: Configured from console by console.

Router-A# pad 2194441 /cud user1 /use-map
Trying 2194441....Open

06:31:12: pad_open_connection: found a matching x25 map pad
06:31:12: Serial1: X.25 O R1 Call (22) 8 lci 1024
06:31:12:   From(7): 2191111 To(7): 2194441
06:31:12:   Facilities: (6)
06:31:12:     Packet sizes: 1024 1024
06:31:12:     Window sizes: 7 7
06:31:12:   Call User Data (12): 0x01000000 (pad)
06:31:12: Serial1: X.25 I R1 Call Confirm (5) 8 lci 1024
06:31:12:   From(0):  To(0):
06:31:12:   Facilities: (0)
06:31:12: PAD0: Call completed
```

Related Commands

Command	Description
show x25 pad	Displays information about current open connections, including packet transmissions, X.3 parameter settings, and the current status of virtual circuits.
translate x25	Automatically translates the request to another outgoing protocol connection type when an X.25 connection request to a particular destination address is received.
x25 map pad	Configures an X.121 address mapping for PAD access over X.25.
x28	Enters X.28 mode and accesses an X.25 network or sets X.3 PAD parameters.

resume (setting X.3 PAD parameters)

To set X.3 parameters, use the **resume** command in EXEC mode.

resume [*connection*] [**/set** *parameter***:***value*]

Syntax Description

connection	(Optional) The name or number of the connection; the default is the most recent connection.
/set *parameter***:***value*	(Optional) Sets the X.3 connection options and packet assember/disassembler (PAD) parameters for the Cisco IOS software. See Table 10 in the Usage Guidelines for the PAD parameter numbers. Refer to the chapter "Configuring the Cisco PAD Facility for X.25 Connections" of the *Cisco IOS Terminal Services Configuration Guide* for a list of these connection options.

Defaults

For outgoing connections, the X.3 parameters default to the following:

```
2:1, 3:2, 4:1, 7:4, 16:127, 17:21, 18:19
```

All other parameters default to zero, but can be changed using the **/set** switch option with either the **resume** command or the **x3** command.

For incoming PAD connections, the software sends an X.29 SET PARAMETER packet to set only the following parameters:

```
2:0, 4:1, 7:21, 15:0
```

Command Modes

EXEC

Command History

Release	Modification
9.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Table 10 summarizes the X.3 PAD Parameters supported on Cisco devices. Refer to the "X.3 PAD Parameters" appendix in the *Cisco IOS Terminal Services Configuration Guide* for more complete information about these parameters.

Table 10 Supported X.3 PAD Parameters

Parameter Number	ITU-T Parameter Name	ITU-T X.3 and Cisco Values
1	PAD recall using a character	Minimum value: 0; maximum value: 126; X.28 PAD user emulation mode default: 1. **Note** Not supported by PAD EXEC user interface.
2	Echo	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode default: 1.
3	Selection of data forwarding character	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 2 (CR); X.28 PAD user emulation mode default: 126 (~).
4	Selection of idle timer delay	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 1; X.28 PAD user emulation mode default: 0.
5	Ancillary device control	Minimum value: 0; maximum value: 2; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 1.
6	Control of PAD service signals	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 2. **Note** Not supported by PAD EXEC user interface.
7	Action upon receipt of a BREAK signal	Minimum value: 0; maximum value: 31; PAD EXEC mode default: 4; X.28 PAD user emulation mode default: 2.
8	Discard output	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
9	Padding after Return	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
10	Line folding	Not supported.
11	DTE speed (binary speed of start-stop mode DTE)	Minimum value: 0; maximum value: 18; PAD EXEC mode and X.28 PAD user emulation mode default: 14.
12	Flow control of the PAD by the start-stop DTE	Minimum value: 0; maximum value: 1; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 1.
13	Line feed insertion (after a Return)	Minimum value: 0; maximum value: 7; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
14	Line feed padding	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
15	Editing	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
16	Character delete	Minimum value: 0; maximum value: 127; PAD EXEC mode and X.28 PAD user emulation mode default: 127 (DEL).
17	Line delete	Minimum value: 0; maximum value: 127; PAD EXEC mode default: 21 (NAK or Ctrl-U); X.28 PAD user emulation mode default: 24 (CAN or Ctrl-X).

Table 10 Supported X.3 PAD Parameters (continued)

Parameter Number	ITU-T Parameter Name	ITU-T X.3 and Cisco Values
18	Line display	Minimum value: 0; maximum value: 127; PAD EXEC mode and X.28 PAD user emulation mode default: 18 (DC2 or Ctrl-R).
19	Editing PAD service signals	Minimum value: 0; maximum value: 126; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 2. **Note** Not supported by PAD EXEC user interface.
20	Echo mask	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0. **Note** Not supported by PAD EXEC user interface.
21	Parity treatment	Minimum value: 0; maximum value: 4; PAD EXEC mode and X.28 PAD user emulation mode default: 0. **Note** For additional values that can be selected for parameter 21, including parity treatment to conform to the French Transpac public switched data network and its technical specification and utilization of networks standards (STUR), see Appendix A, "X.3 PAD Parameters," in the *Cisco IOS Terminal Services Configuration Guide*.

The **/set** switch sets the X.3 parameters defined by parameter number and value, separated by a colon. You set one or more X.3 PAD parameters, as follows:

Step 1 Escape out of the current session by pressing the escape sequence (**Ctrl-Shift-6** then **x** [**Ctrl^x**] by default) and return to the EXEC prompt.

Step 2 Issue the **where** command, to list the open sessions. All open sessions associated with the current terminal line are displayed.

Step 3 Enter the **resume** command, followed by the parameter, a colon, and then the value to be set.

Examples

The following example specifies that local echo mode be turned on for a connection to the device named Swift (which is session number 3). As shown in Table 7, "local echo on" uses the parameter 2 and the value 1 (represented as 2:1 in this example):

```
Swift% ^^X
Router> resume 3 /set 2:1
Swift%
```

Related Commands

Command	Description
where	Lists the open sessions.

resume (switching sessions)

To switch to another open Telnet, rlogin, local-area transport (LAT), or packet assembler/disassembler (PAD) session, use the **resume** command in EXEC mode.

resume [*connection*] [*keyword*] [**/set** *parameter***:***value*]

Syntax Description

connection	(Optional) The name or number of the connection; the default is the most recent connection.
keyword	(Optional) One of the options listed in Table 8.
/set *parameter***:***value*	(Optional) Sets PAD parameters for the Cisco IOS software (see Table 7).

Command Modes

EXEC

Command History

Release	Modification
9.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Table 11 lists Telnet and rlogin resume options.

Table 11 Telnet and rlogin resume Options

Option	Description
/debug	Displays parameter changes and messages. In the Cisco IOS software, this option displays informational messages whenever the remote host changes an X.3 parameter, or sends an X.29 control packet.
/echo	Performs local echo.
/line	Enables line-mode editing.
/nodebug	Cancels printing of parameter changes and messages.
/noecho	Disables local echo.
/noline[1]	Disables line mode and enables character-at-a-time mode, which is the default.
/nostream	Disables stream processing.
/set *parameter:value*	Sets X.3 connection options. Refer to the chapter "Configuring the Cisco PAD Facility for X.25 Connections" of the *Cisco IOS Terminal Services Configuration Guide* for a list of these connection options.
/stream	Enables stream processing.

[1] **/noline** is the default keyword.

You can have several concurrent sessions open and switch between them. The number of sessions that can be open is defined by the **session-limit** command**.**

You can switch between sessions by escaping one session and resuming a previously opened session, as follows:

Step 1 Escape out of the current session by pressing the escape sequence (**Ctrl-Shift-6** then **x** [**Ctrl^x**] by default) and return to the EXEC prompt.

Step 2 Enter the **where** command, to list the open sessions. All open sessions associated with the current terminal line are displayed.

Step 3 Enter the **resume** command and the session number to make the connection.

You also can resume the previous session by pressing the **Return** key.

The **Ctrl^x**, **where**, and **resume** commands are available with all supported connection protocols.

Examples

The following example shows how to escape out of a connection and to resume connection 2:

```
Swift% ^^X
Router> resume 2
```

You can omit the command name and simply enter the connection number to resume that connection. The following example illustrates how to resume connection 3:

```
Router> 3
```

Related Commands

Command	Description
session-limit	Sets the maximum number of terminal sessions per line.
show tn3270 ascii-hexval	Displays ASCII-hexadecimal character mappings.
where	Lists open sessions associated with the current terminal line.

rlogin

To log in to a UNIX host using rlogin, use the **rlogin** command in EXEC mode.

rlogin *host* [**-l** *username*] [**/user** *username*] [**/quiet**] [**debug**]

Syntax Description

host	Specifies the host name or IP address.
-l *username*	(Optional) The Berkeley Standard Distribution (BSD) UNIX syntax that specifies a username for the remote login. If you do not use this option, the remote username is your local username.
/user *username*	(Optional) The EXEC command syntax that specifies a remote username in the initial exchange with the remote host. The rlogin protocol will not present you with the `login` prompt. The **/** character must be entered.
/quiet	(Optional) Prevents onscreen display of all messages from the Cisco IOS software. The **/** character must be entered.
debug	(Optional) Enables debugging output from the rlogin protocol.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.1	The **/quiet** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can have several concurrent rlogin connections open and switch between them. To open a new connection, first suspend the current connection by pressing the escape sequence (**Ctrl-Shift-6** then **x [Ctrl^x**] by default) to return to the EXEC prompt. Then open a new connection. A user cannot automatically log in to a UNIX system from the router, but must provide a user ID and a password for each connection.

If your preferred transport is set to **rlogin**, you can use the **connect** command in place of the **rlogin** command. Refer to the chapter "Configuring Terminal Operating Characteristics for Dial-In Sessions" in the *Cisco IOS Terminal Services Configuration Guide* for more information about configuring a preferred transport type. When your preferred transport is set to **none** or to another protocol, you must use the **rlogin** command to connect to a host.

To terminate an active rlogin session, enter one of the following commands at the UNIX prompt of the device to which you are connecting:

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

- **quit**

Examples

The following example illustrates how a user with the login name jsmith can use the **rlogin ?** help command and the **debug** command mode to establish and troubleshoot a remote connection to the host named Alviso:

```
Router> rlogin ?
  WORD  IP address or hostname of a remote system
Router> rlogin system1 ?
  -l     Specify remote username
  /quiet Suppress login/logout messages
  /user  Specify remote username
  debug  Enable rlogin debugging output
  <cr>
Router> rlogin system1 -l ?
  WORD  Remote user name
Router> rlogin system1 -l username?
 debug Enable rlogin debugging output
  <cr>
Router> rlogin system1 -l username debug
```

The following example illustrates debug return on the host named router1 by the user named user1:

```
Router# rlogin router1.cisco.com -l staff debug
Trying router1.cisco.com (171.69.63.31)... Open
RLOGIN: local username is: ciscoTS
RLOGIN: remote username is: user1
Password:
Last login: Wed Jun 24 06:15:36 from itech-view3.cisc
1 zipper> uptime
  1:40pm  up 42 day(s), 20:53,  80 users,  load average: 1.44, 2.67, 3.39
2 zipper> logout
[Connection to router1.cisco.com closed by foreign host]
Router#
```

The following example makes an rlogin connection to a host at address 10.30.21.2 for a user named user2 and enables the message mode for debugging:

```
Router> rlogin 10.30.21.2 -l user2 debug
```

The following example makes an rlogin connection to a host named headquarters for the user named admin:

```
Router> rlogin headquarters -l admin
```

The following example suppresses all onscreen messages from the Cisco IOS software during login and logout:

```
Router> rlogin host2 /quiet
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
telnet	Logs in to a host that supports Telnet.

rlogin trusted-localuser-source

To choose an authentication method for determining the local username to send to the remote rlogin server, use the **rlogin trusted-localuser-source** command in global configuration mode. To restore the default rlogin behavior, use the **no** form of this command.

rlogin trusted-localuser-source [**local** | **radius** | **tacacs**]

no rlogin trusted-localuser-source [**local** | **radius** | **tacacs**]

Syntax Description

local	(Optional) Uses local username from any authentication method.
radius	(Optional) Uses local username from RADIUS authentication.
tacacs	(Optional) Uses local username from TACACS authentication.

Defaults

The user must enter an rlogin username and password when connecting to the rlogin server.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to define which of the sources for local usernames are valid.

The rlogin protocol passes three types of information: the remote username, the local username, and the local host name of the router. The **rlogin trusted-localuser-source** command allows you to configure one of three behaviors for making connections to the rlogin server, as follows:

- The user must enter a login username and password to connect (default).
- The Cisco IOS-authenticated username can be passed to the rlogin server so the user need only enter a password to connect.
- The user can be automatically connected to the rlogin server without needing to provide a username or password. This configuration is made by using both the **rlogin trusted-localuser-source** and **rlogin trusted-remoteuser-source local** commands where both the Cisco IOS authenticated username and the rlogin server username are the same.

Examples

The following example uses the local username from RADIUS authentication:

```
Router# configure terminal
Router(config)# rlogin trusted-localuser-source ?
  local   Use local username from any authentication method
  radius  Use local username from radius authentication
  tacacs  Use local username from tacacs authentication
Router(config)# rlogin trusted-localuser-source radius
```

Related Commands

Command	Description
ip alias	Assigns an IP address to the service provided on a TCP port.
retry keepalive	Logs in to a UNIX host using rlogin.
rlogin trusted-remoteuser-source local	Determines the remote username to send to the remote rlogin server.
template	Temporarily defines the list of services to which you or another user can connect.

rlogin trusted-remoteuser-source local

To determine the remote username to send to the remote rlogin server, use the **rlogin trusted-remoteuser-source local** command in global configuration mode. To restore the default rlogin behavior, which is to prompt the user for the remote username, use the **no** form of this command.

rlogin trusted-remoteuser-source local

no rlogin trusted-remoteuser-source local

Syntax Description

This command has no arguments or keywords.

Defaults

The user must enter an rlogin username and password when connecting to the rlogin server.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The current username is used only if the **rlogin** *host* **/user** *username* command is not enabled. If the current username is not known, rlogin falls back to providing the “login:” prompt to discover a remote username.

After you issue the **rlogin trusted-remoteuser-source local** command, you will not be prompted for a username. The first response you see is the password prompt from the remote system. For example, when this command is not enabled, you must enter your username twice (once at initial system login and once for the **rlogin** command).

Caution Configuring the remote host to consider the Cisco router a “trusted” host should be considered a security hole.

Examples

The following sample output shows the two prompts a user must reply to when the **rlogin trusted-remoteuser-source local** command is not set:

```
User Access Verification

Username: user1
Password: xxxxx

Router> rlogin router
Trying router.cisco.com (172.16.3.154)... Open
```

```
login: user1
Password: xxxxx
```

The following example shows that after you issue the **rlogin trusted-remoteuser-source local** command, you no longer need to specify the username after the **rlogin** command. The username is automatically copied from the user ID of the router:

```
Router# enable
Password: xxxxx
Router# configure terminal
Router(config)# rlogin ?
  trusted-localuser-source   Allowed authentication types for local username
  trusted-remoteuser-source  Method used to get remote username
Router(config)# rlogin trusted-remoteuser-source local
Router(config)# ^Z
Router# rlogin router
Trying router.cisco.com (172.16.3.154)... Open
Password: xxxxx
```

The following example uses the **/user root** keyword option as an override:

```
Router# rlogin router /user root
Trying router.cisco.com (172.16.3.154)... Open
Password: xxxxx
login:
```

Related Commands

Command	Description
ip alias	Assigns an IP address to the service provided on a TCP port.
retry keepalive	Logs in to a UNIX host using rlogin.
rlogin trusted-localuser-source	Chooses an authentication method for determining the local username to send to the remote rlogin server.
template	Temporarily defines the list of services to which you or another user can connect.

rsa keypair-name

To name the Rivest, Shamir, and Adelman (RSA) keypair to be used for a persistent Secure Shell (SSH) connection, use the **rsa keypair-name** command in transport map configuration mode command. To restore the default setting of no configured RSA keypair name, use the **no** form of the command.

rsa keypair-name *rsa-keypair-name*

no rsa keypair-name

Syntax Description

rsa-keypair-name	The name of the RSA keypair to be used for a persistent SSH connection.

Command Default

No RSA keypair names for persistent SSH are specified by default.

Command Modes

Transport map configuration (config-tmap)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

For persistent SSH connections, the RSA keypair name must be defined using this command in transport map configuration mode. The RSA keypair definitions defined elsewhere on the router, such as through the use of the **ip ssh rsa keypair-name** command, do not apply to persistent SSH connections.

The generation of an RSA keypair, by default, starts the IOS internal SSH server. If you do not want to generate an SSH keypair using IOS, configure the **ip ssh rsa keypair-name** as a value that would never generate a connection (such as **ip ssh rsa keypair-name none**, **ip ssh rsa keypair-name never**, or any other name that will never generate a connection)

Examples

In the following example, a transport map that will make all SSH connections wait for the IOS process to become active before connecting to the router is configured and applied to the Management Ethernet interface (interface gigabitethernet 0). The RSA keypair is named “sshkeys”.

This example only uses the commands required to configure persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 0
```

In the following example, a transport map is configured that applies the following settings to any users attempting to access the Management Ethernet port via SSH:

- Users using SSH wait for the IOS process to become active, but enter diagnostic mode if the attempt to access IOS is interrupted.
- The RSA keypair name is “sshkeys”

- The connection allows one authentication retry.
- The banner “--Welcome to Diagnostic Mode--” appears if diagnostic mode is entered as a result of SSH handling through this transport map.
- The banner “--Waiting for IOS Process--” appears if the connection is waiting for the IOS process to be come active.

The transport map is then applied to the interface when the **transport type persistent ssh input** command is entered to enable persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptable
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# authentication-retries 1
Router(config-tmap)# banner diagnostic X
Enter TEXT message.  End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message.  End with the character 'X'.
--Waiting for IOS Process--
X
Router(config-tmap)# time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit

Router(config)# transport type persistent ssh input sshhandler
```

Related Commands

Command	Description
authentication-retries	Specifies the number of SSH authentication retries before dropping the connection when a persistent SSH transport map is applied to the receiving interface.
banner (transport map)	Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS process as a result of the transport map configuration.
connection wait	Specifies how an incoming connection will be handled.
time-out	Specifies the SSH timeout interval in seconds.
transport interface	Applies the transport map settings to the interface.
transport type persistent	Applies an already-configured persistent transport map to an interface.
transport-map type persistent	Creates and names a persistent transport map and enters transport map configuration mode.

rxspeed

To set the terminal receive speed (how fast the terminal receives information from the modem), use the **rxspeed** command in line configuration mode. To reset the default value, use the **no** form of this command.

rxspeed *bps*

no rxspeed

Syntax Description

bps	Baud rate in bits per second (bps). The default value is 9600 bps.

Defaults

9600 bps

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Set the speed to match the baud rate of whatever device you have connected to the port. Some baud rates available on devices connected to the port might not be supported on the system. The system will indicate if the speed you select is not supported.

Note If the line was previously configured for automatic baud rate detection (autobaud), disable autobaud by entering the **no autobaud** command before entering the **rxspeed** command to fix the speed of the port.

Examples

The following example sets the line 5 receive rate to 2400 bps:

```
line 5
 rxspeed 2400
```

Related Commands

Command	Description
source template	Sets the flow control start character.
terminal rxspeed	Sets the terminal receive speed (how fast information is sent to the terminal) for the current line and session.
txspeed	Sets the terminal transmit speed (how fast the terminal sends information to the modem).