

slip

To start a serial connection to a remote host by using Serial Line Internet Protocol (SLIP), use the **slip** command in EXEC mode.

```
slip [/default] {remote-ip-address | remote-name} [@tacacs-server] [/routing] [/compressed]
```

Syntax Description		
/default	(Optional) Makes a SLIP connection when a default address has been configured.	
<i>remote-ip-address</i>	IP address of the client workstation or PC.	
<i>remote-name</i>	Name of the client workstation or PC.	
<i>@tacacs-server</i>	(Optional) IP address or IP host name of the TACACS server to which your TACACS authentication request is sent.	
/routing	(Optional) Indicates that the remote system is a router. Line must be configured for asynchronous routing using SLIP encapsulation.	
/compressed	(Optional) Indicates that IP header compression should be negotiated.	

Command Modes	
EXEC	

Command History	Release	Modification
	10.0	This command was introduced in a release prior to Cisco IOS Release 10.0.

Usage Guidelines

When you connect from a remote node computer to the EXEC facility on a router and want to connect from the router to a device on the network, issue the **slip** command.

If you specify an address for the TACACS server by using **/default** or *tacacs-server* options, the address must be the first parameter in the command after you enter **slip**. If you do not specify an address or enter **/default**, you are prompted for an IP address or host name. You can enter the **/default** keyword at this point.

If you do not use the *tacacs-server* argument to specify a TACACS server for SLIP address authentication, the TACACS server specified at login (if any) is used for the SLIP address query.

To optimize bandwidth on a line, SLIP enables compression of the SLIP packets using Van Jacobson TCP header compression as defined in RFC 1144.

Your system administrator must configure the system with the **ip tcp header-compression passive** command for the **/compressed** command option to be valid in EXEC mode. The **ip tcp header-compression** command forces header compression on or off. The default is to not compress the packets. The configuration file must have header compression on and the **slip /compressed** EXEC command must be entered for header compression to occur.

To terminate a session initiated with the slip command, disconnect from the device on the network using the command specific to that device. Then, exit from the EXEC by using the **exit** command.

Examples

The following example makes a connection when a default IP address is assigned. Once a correct password is entered, you are placed in SLIP mode, and the IP address is displayed.

```
router> slip
Password:
Entering SLIP mode.
Your IP address is 192.31.7.28, MTU is 1524 bytes
```

The following example illustrates the prompts displayed and the response required when you use dynamic addressing to assign the SLIP address:

```
router> slip
IP address or hostname? 192.31.6.15
Password:
Entering SLIP mode
Your IP address is 192.31.6.15, MTU is 1524 bytes
```

In the preceding example, the address 192.31.6.15 has been assigned as the default. Password verification is still required before SLIP mode can be enabled.

```
router> slip /default
Password:
Entering SLIP mode
Your IP address is 192.31.6.15, MTU is 1524 bytes
```

The following example illustrates the implementation of header compression on the interface with the IP address 128.66.2.1:

```
router> slip 128.66.2.1 /compressed
Password:
Entering SLIP mode.
Interface IP address is 128.66.2.1, MTU is 1500 bytes.
Header compression will match your system.
```

In the preceding example, the interface is configured for the **ip tcp header-compression passive** command, which permits the user to enter the **/compressed** keyword at the EXEC mode prompt. The message “Header compression will match your system” indicates that the user specified compression. If the line was configured for the **ip tcp header-compression on** command, this line would read “Header compression is On.”

The following example specifies a TACACS server named server1 for address authentication:

```
router> slip 1.0.0.1@server1
Password:
Entering SLIP mode.
Interface IP address is 1.0.0.1, MTU is 1500 bytes
Header compression will match your system.
```

snapshot client

To configure a client router for snapshot routing, use the **snapshot client** command in interface configuration mode. Use the **no** form of this command to disable a client router.

snapshot client *active-time quiet-time* [**suppress-statechange-updates**] [**dialer**]

no snapshot client *active-time quiet-time* [**suppress-statechange-updates**] [**dialer**]

Syntax Description	Description
<i>active-time</i>	Amount of time, in minutes, that routing updates are regularly exchanged between the client and server routers. This can be an integer in the range 5 to 100. There is no default value. A typical value is 5 minutes.
<i>quiet-time</i>	Amount of time, in minutes, that routing entries are frozen and remain unchanged between active periods. Routes are not aged during the quiet period, so they remain in the routing table as if they were static entries. This argument can be an integer from 8 to 100000. There is no default value. The minimum quiet time is generally the active time plus 3.
suppress-statechange-updates	(Optional) Disables the exchange of routing updates each time the line protocol goes from “down” to “up” or from “dialer spoofing” to “fully up.”
dialer	(Optional) Used if the client router has to dial up the remote router in the absence of regular traffic.

Defaults

Snapshot routing is disabled.

The *active-time* and *quiet-time* arguments have no default values.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The value of the *active-time* argument must be the same for the client and server routers.

To specify the remote server routers to be called by this client router during each active period, use the **dialer map snapshot** command.

Examples

The following example configures a client router for snapshot routing:

```
interface dialer 1
 snapshot client 5 600 suppress-statechange-updates dialer
```

Related Commands	Command	Description
	clear resource-pool	Ends the quiet period on a client router within 2 minutes.
	snapshot client	Configures a client router for snapshot routing.
	show snapshot	Displays snapshot routing parameters associated with an interface.
	snapshot server	Configures a server router for snapshot routing.

snapshot server

To configure a server router for snapshot routing, use the **snapshot server** command in interface configuration mode. Use the **no** form of this command to disable a server router.

snapshot server *active-time* [**dialer**]

no snapshot server *active-time* [**dialer**]

Syntax Description		
	<i>active-time</i>	Amount of time, in minutes, that routing updates are regularly exchanged between the client and server routers. This can be an integer in the range 5 to 100. There is no default value. A typical value is 5 minutes.
	dialer	(Optional) Allows the client router to dial up the remote router in the absence of regular traffic.

Defaults

Snapshot routing is disabled.
The *active-time* argument has no default value.

Command Modes

Interface configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines

The value of the *active-time* argument must be the same for the client and server routers.

Examples

The following example configures a server router for snapshot routing:

```
interface dialer 1
 snapshot server 5
```

Related Commands	Command	Description
	show snapshot	Displays snapshot routing parameters associated with an interface.
	snapshot client	Configures a client router for snapshot routing.

source template

To attach a configured customer profile template to a particular customer profile, use the **source template** command in customer profile configuration mode.

source template *name*

Syntax Description	<i>name</i> Customer profile template name.
---------------------------	---

Defaults No templates are sourced or attached to a customer profile.

Command Modes Customer profile configuration

Command History	Release	Modification
	12.0(6)T	This command was introduced.

Usage Guidelines All PPP and peer-default commands are allowed for a particular customer profile template under this grouping.

Examples The following example shows the creation and configuration of a customer profile template named acme-direct and its subsequent assignment to the customer profile acme1:

```
template acme-direct
 multilink {max-fragments num | max-links num | min-links num}
 peer match aaa-pools
 peer default ip address pool acme-numbers
 ppp ipcp dns 10.1.1.1 10.2.2.2
 ppp multilink
 exit
 resource-pool profile customer acme1
 source template acme-direct
```

Related Commands	Command	Description
	template	Accesses the template configuration mode for configuring a particular customer profile template.

source-ip

To specify an alternate IP address for a Virtual Private Dialup Network (VPDN) tunnel that is different from the physical IP address used to open the tunnel, use the **source-ip** command in VPDN group configuration mode. To remove the alternate IP address, use the **no** form of this command.

source-ip *ip-address*

no source-ip

Syntax Description	<i>ip-address</i>	Alternate IP address (different from the physical IP address used to open the VPDN tunnel) that the router uses to identify the tunnel.
---------------------------	-------------------	---

Defaults	Disabled
-----------------	----------

Command Modes	VPDN group configuration
----------------------	--------------------------

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines	Each VPDN group on a router can be configured with a unique source-ip command.
-------------------------	---

Examples	The following example configures a LAC to accept L2TP dialout calls using the alternate IP address 172.23.33.7, which is different from the physical IP address used to open the L2TP tunnel:
-----------------	---

```
vpdn-group 3
  accept-dialout
    protocol l2tp
    dialer 2
  terminate-from hostname orpheus
  source-ip 172.23.33.7
```

Related Commands	Command	Description
	accept dialin	Specifies the LNS to use for authenticating, and the virtual template to use for cloning, new virtual access interfaces when an incoming L2TP tunnel connection is requested from a specific peer.
	accept dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup.
	request dialin	Configures a VPDN group to request L2F or L2TP tunnels to a home gateway and creates a request-dialin VPDN subgroup.
	request dialout	Enables an LNS to request VPDN dial-out calls by using L2TP.

spe

To access the SPE configuration mode and control the downloading of firmware into the modems, use the **spe** command in global configuration mode. There is no **no** version of this command.

```
spe {shelf/slot/module} {shelf/slot/module}
```

Syntax Description

shelf/slot/module Enter the shelf number, slot number, and module number separated by slashes, as shown. For Cisco AS5200 and AS5300, enter only the slot/module.

To specify a range of modems when this option is selected as a start point, use the following set of arguments as an endpoint.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI1	This command was introduced.
12.0(5)T	This document changed to reflect new information on the command.

Usage Guidelines

The **spe** global configuration command enables the SPE configuration mode. Configure your SPE by specifying a slot and an SPE associated with the slot; or, you can configure a range of SPEs by specifying the first and last SPE in the range. On AS5800 platforms, you must also specify the shelf associated with the slot and SPE.

When the access server is booted, the **spe** global configuration command specifies the location from where the firmware image is downloaded to the SPE. If the **spe** configuration command is used to download the firmware from flash memory and then subsequently the **no** version of the exact command is entered, then the **spe** command downloads the embedded firmware.

The **spe** command was first supported in Cisco IOS Release 12.0(4)XI1 along with the Resource Pool Management feature (although it can be used independently). For earlier images, use the **copy** command on the Cisco AS5200 and Cisco AS5300, and the **modem-pool** command on the Cisco AS5800. For the Cisco IOS Release 12.0(5)T images, the **copy {flash | system | tftp} modem** command will be disabled for firmware and newer version of Microcom modems (i.e., 56Kbps). Old V.34 Microcom modems still use the **copy** command for downloading in Cisco IOS Release 12.0(5)T images. For Cisco AS5800, downloading firmware through the **modem-pool** command is disabled.



Note

Use this command when traffic is low since the **spe** download does not begin until the modems have no active calls.

**Note**

The **spe** command is a configuration command—save it using the **write memory** command, otherwise the configuration will not be saved. If the configuration is not saved, the downloading of the specified firmware will not occur after the next reboot.

Examples

The following example shows the **spe** command being used from global configuration mode to access the SPE configuration mode for the SPE range from 1/2 to 1/4:

```
spe 1/2 1/4
```

Related Commands

Command	Description
request dialin	Configures a VPDN group to request L2F or L2TP tunnels to a home gateway and creates a request-dialin VPDN subgroup.
firmware location	Downloads a firmware image to a modem (SPE configuration).

spe recovery

To set a service processing element (SPE) port for recovery, use the **spe recovery** command in global configuration mode. To disable SPE recovery or to restore the default **port-threshold** value, use the **no** form of this command.

```
spe recovery {port-action {disable | recover} | port-threshold number-failures}
```

```
no spe recovery {port-action | port-threshold}
```

Syntax Description

port-action	Action to apply to the port for recovery when the configured port-threshold value has been exceeded.
disable	Sets the port to the bad state.
recover	Sets the port for recovery.
port-threshold <i>number-failures</i>	Number of consecutive failed attempts made on the port before the port-action keyword is applied. The range is from 1 to 10000. The default value is 30.

Defaults

There is no default **port-action** value. SPE recovery is disabled.
The default **port-threshold** value is 30 failed attempts.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(2.3)T1	This command was implemented on the Cisco AS5800.

Usage Guidelines

Failure of an SPE port to connect after repeated tries indicates that a problem exists in the SPE or firmware. An SPE port in this state is recovered by downloading firmware.

When an SPE port fails to connect consecutively for a number of times, as specified by the **port-threshold** *number-failures* keyword and argument, the SPE is moved to a state based on the **port-action** configuration.

If the **spe recovery port-action recover** command has been configured, when the **port-threshold** *number-failures* value is exceeded, the port is temporarily marked as disabled (“d” state) to avoid further incoming calls, and it is then marked for recovery (“r” state). Any SPE that has a port marked for recovery will download firmware when the SPE is idle (when none of the ports on the SPE have active calls).

If the **spe recovery port-action disable** command has been configured, when the **port-threshold** *number-failures* value is exceeded, the port is marked as bad (“BAD” state). An SPE with a port that is marked as bad must be explicitly cleared in order for that port to be used again.

If no **port-action** is configured, the port will be marked as not in use (“_” state). An SPE with a port marked as not in use will remain unusable until it is explicitly cleared, and the SPE will not accept incoming calls on any of the ports.

SPE recovery can be disabled by issuing the **no spe recovery port-action** command. If SPE recovery is disabled, the SPE will behave as if no **port-action** has been configured.

**Note**

Beginning with Cisco IOS Release 12.1(2.3)T1, the modem recovery action for MICA technologies modems on the Cisco AS5800 platforms is done using the **spe recovery** command rather than the **modem recovery** command.

Examples

The following example configures the SPE to recover ports that exceed the call failure threshold:

```
Router(config)# spe recovery port-action recover
```

The following example sets a value of 50 for the number of consecutive failed attempts on the port before the **port-action** keyword is applied:

```
Router(config)# spe recovery port-threshold 50
```

Related Commands

Command	Description
clear port	Resets the NextPort port and clears any active call.
clear spe	Reboots all specified SPEs.
firmware upgrade	Specifies an SPE firmware upgrade method.
show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe version	Displays the firmware version on an SPE and displays the version to firmware file mappings.
spe download maintenance	Performs download maintenance on SPEs that are marked for recovery.

start-character

To set the flow control start character, use the **start-character** command in line configuration mode. Use the **no** form of this command to remove the character.

start-character *ascii-number*

no start-character

Syntax Description	<i>ascii-number</i>	Decimal representation of the start character.
--------------------	---------------------	--

Defaults	Decimal 17
----------	------------

Command Modes	Line configuration
---------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	This command defines the character that signals the start of data transmission when software flow control is in effect. Refer to the “ASCII Character Set” appendix in the <i>Cisco IOS Configuration Fundamentals Command Reference</i> for a list of ASCII characters.
------------------	--

Examples	The following example changes the start character to Ctrl-B, which is decimal 2:
----------	--

```
line 2
 start-character 2
```

Related Commands	Command	Description
	flowcontrol	Sets the method of data flow control between the terminal or other serial device and the router.
	stop-character	Sets the flow control stop character.
	terminal start-character	Changes the flow control start character for the current session.

start-chat

To specify that a chat script start on a specified line at any point, use the **start-chat** command in privileged EXEC mode. Use the **no** form of this command to stop the chat script.

start-chat *regexp* [*line-number* [*dialer-string*]]

no start-chat

Syntax Description		
<i>regexp</i>		Specifies the name of a regular expression or modem script to be executed. If there is more than one script with a name that matches the argument <i>regexp</i> , the first script found will be used.
<i>line-number</i>		(Optional) Indicates the line number on which to execute the chat script. If you do not specify a line number, the current line number is chosen. If the specified line is busy, the script is not executed and an error message appears. If the dialer-string argument is specified, line-number must be entered; it is not optional if you specify a dialer string. This command functions only on physical terminal (TTY) lines. It does not function on virtual terminal (VTY) lines.
<i>dialer-string</i>		(Optional) String of characters (often a telephone number) to be sent to a DCE. If you enter a dialer string, you must also specify <i>line-number</i> , or the chat script <i>regexp</i> will not start.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines

This command provides modem dialing commands for a chat script that you want to apply immediately to a line. If you do not specify a line, the script runs on the current line. If the specified line is already in use, the script is not activated and an error message appears.

The argument *regexp* is used to specify the name of the modem script that is to be executed. The first script that matches the argument in this command and the **dialer map** command will be used. For more information about regular expressions, refer to the “Regular Expressions” appendix in this publication.

This command functions only on physical terminal (TTY) lines. It does not function on virtual terminal lines.

Examples The following example forces a dialout on line 8 using the script telebit:

```
start-chat telebit line 8
```

Related Commands	Command	Description
	chat-script	Places calls over a modem and logs in to remote systems.
	dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites
	script activation	Specifies that a chat script start on a physical terminal line when the line is activated.
	script connection	Specifies that a chat script start on a physical terminal line when a remote network connection is made to a line.
	script dialer	Specifies a default modem chat script.
	script reset	Specifies that a chat script start on a physical terminal line when the specified line is reset.
	script startup	Specifies that a chat script start on a physical terminal line when the router is powered up.

stop-character

To set the flow control stop character, use the **stop-character** command in line configuration mode. Use the **no** form of this command to remove the character.

stop-character *ascii-number*

no stop-character

Syntax Description	<i>ascii-number</i>	Decimal representation of the stop character.
---------------------------	---------------------	---

Defaults	Decimal 19
-----------------	------------

Command Modes	Line configuration
----------------------	--------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	This command defines the character that signals the end of data transmission when software flow control is in effect. Refer to the “ASCII Character Set” appendix in the <i>Cisco IOS Configuration Fundamentals Command Reference</i> for a list of ASCII characters.
-------------------------	--

Examples	The following example changes the stop character to Ctrl-E, which is decimal 5:
-----------------	---

```
line 3
 stop-character 5
```

Related Commands	Command	Description
	flowcontrol	Sets the method of data flow control between the terminal or other serial device and the router.
	source template	Sets the flow control start character.
	stop-character	Sets the flow control stop character.

telnet

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

```
telnet host [port] [keyword]
```

Syntax Description	host	A host name or an IP address.
	port	(Optional) A decimal TCP port number; the default is the Telnet router port (decimal 23) on the host.
	keyword	(Optional) One of the keywords listed in Table 126.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.1	The /quiet keyword was added.

Usage Guidelines Table 126 lists the optional **telnet** command keywords.

Table 133 telnet Command 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).
/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 <i>path</i> argument is a list of host names or IP addresses that specify network nodes and ends with the final destination.
/source-interface	Specifies the source interface.

Table 133 telnet Command Keyword Options (continued)

Option	Description
<i>/stream</i>	Turns on <i>stream</i> processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running Unix-to-Unix Copy Program (UUCP) and other non-Telnet protocols.
<i>port-number</i>	Port number.
bgp	Border Gateway Protocol.
chargen	Character generator.
cmd <i>rcmd</i>	Remote commands.
daytime	Daytime.
discard	Discard.
domain	Domain Name 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.
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.

Table 133 telnet Command Keyword Options (continued)

Option	Description
whois	Nickname.
www	World Wide Web.

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

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

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

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

The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is **Ctrl-^** (press and hold the **Ctrl** and **Shift** keys and the **6** key). You can enter the command character as you hold down **Ctrl** or with **Ctrl** released; you can use either uppercase or lowercase letters. Table 127 lists the special Telnet escape sequences.

Table 134 Special Telnet Escape Sequences

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

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

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

Ctrl-^ ?

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

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

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

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

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

Examples

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

```
router> telnet host1 /encrypt kerberos
```

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

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

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

```
router> host1
```

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

```
router> telnet 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
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
kerberos clients mandatory	Causes the rsh , rcp , rlogin , and telnet commands to fail if they cannot negotiate the Kerberos Protocol with the remote server.
rlogin	Logs in to a UNIX host using rlogin.

telnet break-on-ip

To cause the system to generate a hardware BREAK signal on the EIA/TIA-232 line that is associated with a reverse Telnet connection when a Telnet Interrupt-Process command is received on that connection, use the **telnet break-on-ip** command in line configuration mode.

telnet break-on-ip

Syntax Description

This command has no arguments or keywords.

Defaults

No hardware Break signal is generated when an Interrupt-Process command is received.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command causes the system to generate a hardware BREAK signal on the RS-232 line that is associated with a reverse Telnet connection. It is useful when a Telnet Interrupt-Process command is received on that connection because it can control the translation of Telnet Interrupt-Process commands into X.25 BREAK indications. It is also a useful workaround in the following situations:

- Several user Telnet programs send an Interrupt-Process command, but cannot send a Telnet BREAK signal.
- Some Telnet programs implement a BREAK signal that sends an Interrupt-Process command.
- Some EIA/TIA-232 hardware devices use a hardware BREAK signal for various purposes.

A hardware BREAK signal is generated when a Telnet BREAK command is received.

Examples

In the following example, line 5 is configured with the **telnet break-on-ip** command. The location text notes that this refers to the high-speed modem. The **telnet transparent** command sets end-of-line handling.

```
line 5
 location high-speed modem
 telnet transparent
 telnet break-on-ip
```

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.
	telnet transparent	Configures the Cisco IOS software to send a CARRIAGE RETURN (CR) as a CR followed by a NULL instead of a CR followed by a LINE FEED (LF).
	terminal telnet break-on-ip	Causes the access server to generate a hardware Break signal on the EIA/TIA-232 line, which is associated with a reverse Telnet connection, for the current line and sessions.

telnet refuse-negotiations

To set a line using Telnet to refuse to negotiate full-duplex, remote echo requests on incoming connections, use the **telnet refuse-negotiations** command in line configuration mode.

telnet refuse-negotiations

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Line configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Use this command on reverse Telnet connections to allow the Cisco IOS software to refuse full-duplex, remote echo option connection requests from the other end. This command suppresses negotiation of the Telnet Remote Echo and Suppress Go Ahead options.

This command does not apply to protocol translation configurations. It is intended for applications wherein the router is functioning as a terminal server to allow terminal connections to remote devices through the asynchronous terminal ports of the router. Terminal server connections are those where the user types a command similar to the following to access network resources:

```
telnet access-server 2005
```

where access-server is the host name of the Cisco router functioning as a terminal server, and 2005 is the port number on the router to which the remote terminal is connected.

Examples The following example shows how to set line 5 to refuse full-duplex, remote echo requests:

```
line 5
telnet refuse-negotiations
```

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.
	terminal telnet refuse-negotiations	Sets the current line to refuse to negotiate full-duplex, remote echo options on incoming connections for current sessions.

telnet speed

To allow the Cisco IOS software to negotiate transmission speed of the line to a connected device, use the **telnet speed** command in line configuration mode.

telnet speed *default-speed maximum-speed*

Syntax Description		
<i>default-speed</i>	Line speed (in bps) that the Cisco IOS software will use if the device on the other end of the connection has not specified a speed.	
<i>maximum-speed</i>	Maximum speed (in bps) that the device on the port will use.	

Defaults No default behavior or values.

Command Modes Line configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Negotiates speeds on reverse Telnet lines. You can match line speeds on remote systems in reverse Telnet, on host machines hooked up to a router used to access the network, or on a group of console lines hooked up to the router, when disparate line speeds are in use at the local and remote ends of the connection. Line speed negotiation adheres to the Remote Flow Control option, defined in RFC 1080.

Examples The following example allows a router to negotiate a bit rate on the line using the Telnet option. If no speed is negotiated, the line will run at 2400 bits per second. If the remote host requests a speed of greater than 9600 bps, then 9600 will be used.

```
line 5
telnet speed 2400 9600
```

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.
	terminal telnet speed	Allows the access server to negotiate transmission speed for the current line and session.

telnet sync-on-break

To configure the Cisco IOS software to cause an incoming connection to send a Telnet Synchronize signal when it receives a Telnet BREAK signal, use the **telnet sync-on-break** command in line configuration mode.

telnet sync-on-break

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Line configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command causes a reverse Telnet line to send a Telnet Synchronize signal when it receives a Telnet BREAK signal. This option is used very rarely to ensure the ordering of BREAK reception with respect to data characters sent after the BREAK.

Examples The following example configures line 8 with the **telnet sync-on-break** command:

```
line aux 0
telnet sync-on-break
```

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.
	terminal telnet sync-on-break	Causes the access server to send a Telnet Synchronize signal when it receives a Telnet Break signal on the current line and session.

telnet transparent

To configure the Cisco IOS software to send a CARRIAGE RETURN (CR) as a CR followed by a NULL instead of a CR followed by a LINE FEED (LF), use the **telnet transparent** command in line configuration mode.

telnet transparent

Syntax Description This command has no arguments or keywords.

Defaults CARRIAGE RETURN followed by a LINE FEED.

Command Modes Line configuration

Command History	Release	Modification
	10.0	This command was introduced.

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

Examples The following example causes the Cisco IOS software, when sending a CR, to send a CR followed by a NULL character:

```
line 7
telnet transparent
```

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.
	terminal telnet transparent	Causes the current terminal line to send a Return character (CR) as a CR followed by a NULL instead of a CR followed by a Line Feed (LF) for the current session.

template

To access the template configuration mode for configuring a particular customer profile template, use the **template** command in global configuration mode. Use the **no** form of this command to delete the template of the specified name.

```
template name {default | exit | multilink | no | peer | ppp}
```

```
no template name {default | exit | multilink | no | peer | ppp}
```

Syntax Description

<i>name</i>	A name that identifies the template.
default	Sets the command to its defaults.
exit	Exits from resource-manager configuration mode.
multilink	Configures multilink parameters.
no	Negates the command or its defaults.
peer	Accesses peer parameters for point-to-point interfaces.
ppp	Accesses Point-to-Point Protocol.

Defaults

No templates are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

All PPP and peer-default commands are enabled for a customer profile template under this grouping.

Examples

The following example shows the creation and configuration of a customer profile template named acme-direct and its subsequent assignment to the customer profile acme1:

```
template acme-direct
  multilink max-fragments 10
  peer match aaa-pools
  peer default ip address pool acme-numbers
  ppp ipcp dns 10.1.1.1 10.2.2.2
  ppp multilink
  exit
resource-pool profile customer acme1
source template acme-direct
```

■ **template****Related Commands**

Command	Description
source template	Attaches a configured customer profile template to a customer profile.

terminal lat

To temporarily define the list of services to which you or another user can connect, use the **terminal lat** command in EXEC mode.

terminal lat remote-modification

terminal lat out-group *group_number* [*start-end*] { **disabled** | **enabled** }

Syntax Description

remote-modification	Sets the line to be remotely modifiable.
out-group	Defines a group list for outgoing user-initiated connections.
<i>group_number</i>	Number of the group that has access to the system through the specified line. This number is identified by the system administrator. You also can specify a range of group numbers. Separate the beginning and end of the range with a hyphen.
[<i>start-end</i>]	(Optional) You also can specify a range of group numbers with the <i>group_number</i> . Separate the beginning and end of the range with a hyphen.
disabled	Incrementally removes specified groups from list.
enabled	Incrementally adds specified groups to list.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

To temporarily define the list of services to which you or another user can connect, you define the group code lists used for connections from specific lines. You limit the connection choices for an individual line by defining the group code lists for an outgoing connection. When a user initiates a connection with a LAT host, the user's line must share a common group number with the remote LAT host before a connection can be made.

The group code range entered in this command must fall within the group code range already configured for the line.

Examples

The following example defines a group code list for the outgoing group 4:

```
terminal lat out-group 4, 6-189
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
l2f	Specifies a connection to a particular LAT node that offers LAT services.
ignore-mid-sequence	

terminal transport preferred

To specify the preferred protocol to use for the current session when a command does not specify one, use the **terminal transport preferred** command in EXEC mode.

terminal transport preferred { **all** | **lat** | **mop** | **nasi** | **none** | **pad** | **rlogin** | **telnet** | **v120** }

Syntax Description

all	Specifies all recognized protocols.
lat	Specifies the LAT protocol.
mop	Specifies the Maintenance Operation Protocol (MOP).
nasi	Specifies the NetWare Asynchronous Services Interface (NASI) protocol.
none	Prevents any protocol selection on the line. The router default is that any unrecognized command is a host name. If the preferred protocol is set to none, the router will not attempt any connections if the command is not recognized.
pad	Specifies X.3 PAD, which is used most often to connect a server product to X.25 hosts.
rlogin	Specifies UNIX rlogin.
telnet	Specifies the TCP/IP Telnet protocol.
v120	Selects the V.120 protocol for incoming async over ISDN connections.

Defaults

lat (if LAT is not supported, **telnet**)

Command Modes

EXEC

Command History

Release	Modification
10.0	This command first appeared in a release prior to Cisco IOS Release 10.0.
11.2	The following keywords were added: <ul style="list-style-type: none"> • preferred • all • lat • mop • nasi • pad • rlogin • v120

Examples

The following example configures the console so that it does not connect when an unrecognized command is entered:

```
terminal transport preferred none
```

Related Commands	Command	Description
	transport preferred	Specifies the transport protocol that the Cisco IOS software uses if the user does not specify one when initiating a connection.

terminate-from

To specify the host name of the remote L2TP access concentrator (LAC) or L2TP network server (LNS) that will be required when accepting a Virtual Private Dialup Network (VPDN) tunnel, use the **terminate-from** command in VPDN group configuration mode. To remove the host name from the VPDN group, use the **no** form of this command.

terminate-from *hostname* *hostname*

no terminate-from [*hostname* *hostname*]

Syntax Description	hostname <i>hostname</i> (Optional) The host name that this VPDN group will accept connections from.
---------------------------	---

Defaults	Disabled
-----------------	----------

Command Modes	VPDN group configuration
----------------------	--------------------------

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines	<p>Before you can use this command, you must have already enabled one of the two accept VPDN subgroups by using either the accept dialin or accept dialout command.</p> <p>Each VPDN group can only terminate from a single host name. If you enter a second terminate-from command on a VPDN group, it will replace the first terminate-from command.</p>
-------------------------	--

Examples	<p>The following example configures a VPDN group to accept L2TP tunnels for dialout calls from the LNS cerise by using dialer 2 as its dialing resource:</p>
-----------------	--

```
vpdn-group 1
  accept dialout
  protocol l2tp
  dialer 2
  terminate-from hostname cerise
```

Related Commands	Command	Description
	accept dialin	Specifies the LNS to use for authenticating, and the virtual template to use for cloning, new virtual access interfaces when an incoming L2TP tunnel connection is requested from a specific peer.
accept dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup	

test modem back-to-back

To diagnose an integrated modem that may not be functioning properly, use the **test modem back-to-back** command in EXEC mode.

test modem back-to-back *first-slotport second-slotport*

Syntax Description	<i>first-slotport</i>	Slot and modem number of the first test modem. Remember to include the forward slash (/) when entering this variable.
	<i>second-slotport</i>	Slot and modem number of the second test modem. Remember to include the forward slash (/) when entering this variable.
Defaults	Disabled	
Command Modes	EXEC	
Command History	Release	Modification
	11.2	This command was introduced.
Usage Guidelines	Use this command to perform back-to-back testing of two modems. You might need to enable this command on several different combinations of modems to determine which one is not functioning properly.	
Examples	<p>The following example performs a back-to-back modem test between modem 2/0 and modem 2/1 and removes modem 2/1 (which is associated with TTY line 26) from all dial-in and dial-out services:</p> <pre>router# test modem back-to-back 2/0 2/1 back2back 2/0 2/1 Repetitions (of 10-byte packets) [1]: router# %MODEM-5-B2BCONNECT: Modems (2/0) and (2/1) connected in back-to-back test: CONNECT9600/REL-MNPM %MODEM-5-B2BMODEMS: Modems (2/0) and (2/1) completed back-to-back test: success/packets = 2/2</pre>	
Related Commands	Command	Description
	modem bad	Removes an integrated modem from service and indicates it as suspected or proven to be inoperable.

timeout absolute

To specify a timeout period that controls how long a session can be connected before it is terminated, use the **timeout absolute** interface configuration command. To remove the session timeout period, use the **no** form of this command.

timeout absolute *minutes* [*seconds*]

no timeout absolute

Syntax Description

<i>minutes</i>	Session lifetime in minutes, in the range from 0 to 35790 minutes.
<i>seconds</i>	(Optional) Session lifetime in seconds, in the range from 0 to 59 seconds.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Examples

The following partial example shows how to impose a 15-minute (900-second) idle timeout and a 12-hour (720-minute) absolute timeout for session connections:

```
interface Serial0:23
  dialer idle-timeout 900
  timeout absolute 720
!
interface Serial1:23
  dialer idle-timeout 900
  timeout absolute 720
.
.
.
```

Related Commands

Command	Description
ppp idle timeout	Sets PPP idle timeout parameters.
dialer idle-timeout	Specifies the idle time before the line is disconnected.

tn3270

To begin a TN3270 session, use the **tn3270** command in EXEC mode.

tn3270 *host*

Syntax Description	<i>host</i>	Name or IP address of a specific host on a network that can be reached by the router. The default terminal emulation mode allows access using a VT100 emulation.
---------------------------	-------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines Unlike Telnet and LAT connections, you *must* enter the **tn3270** command to make a connection to an IBM TN3278 host.

To terminate an active TN3270 session, enter the escape sequence (**Ctrl-Shift-6** then **x** [**Ctrl^x**] by default) and enter the **disconnect** command at the EXEC prompt. Or log off the remote system by issuing the command specific to that system (such as **exit**, **logout**, **quit**, **close**, or **disconnect**).

Examples The following example establishes a terminal session with an IBM TN3270 host named finance:

```
tn3270 finance
```

tn3270 8bit display

To configure the Cisco IOS software to use the mask set by the **data-character-bits {7 | 8}** command in line configuration mode or the **terminal data-character bits {7 | 8}** command in EXEC mode, use the **tn3270 8bit display** command in line configuration mode. Use the **no** form of this command to restore the default 7-bit mask used for TN3270 connections.

tn3270 8bit display

no tn3270 8bit display

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.

Usage Guidelines Use the **tn3270-character-map** command to map between extended EBCDIC or extended ASCII characters.

Examples The following example configures the Cisco IOS software to use the mask set by the **data-character-bits** line configuration and EXEC commands on line 5:

```
line 5
tn3270 8bit display
```

Related Commands	Command	Description
	data-character-bits	Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software.
	terminal data-character-bits	Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software for the current line and session.

tn3270 8bit transparent-mode

To configure the Cisco IOS software to use the mask set by the **data-character-bits {7 | 8}** command in line configuration mode or the **terminal data-character bits {7 | 8}** command in EXEC mode, use the **tn3270 8bit transparent-mode** command in line configuration mode. Use the **no** form of this command to restore the default 7-bit mask used for TN3270 connections.

tn3270 8bit transparent-mode

no tn3270 8bit transparent-mode

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.

Usage Guidelines This command is needed if you are using a file transfer protocol such as Kermit in 8-bit mode or you are using 8-bit graphics, both of which rely on transparent mode.

Examples The following example configures the software to use the mask set by the **data-character-bits** line configuration and EXEC commands on line 5:

```
line 5
tn3270 8bit transparent-mode
```

Related Commands	Command	Description
	data-character-bits	Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software.
	terminal data-character-bits	Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software for the current line and session.

tn3270 character-map

To convert incoming EBCDIC characters into ASCII characters, use the **tn3270 character-map** command in global configuration mode. Use the **no** form of this command to restore default character mappings.

```
tn3270 character-map ebcdic-in-hex ascii-in-hex
```

```
no tn3270 character-map {all | ebcdic-in-hex} [ascii-in-hex]
```

Syntax Description

<i>ebcdic-in-hex</i>	Hexadecimal value of an EBCDIC character.
<i>ascii-in-hex</i>	(Optional) Hexadecimal value of an ASCII character.
all	Indicates all character mappings.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to print international characters that are EBCDIC characters not normally printed, including umlauts (¨) and tildes (~). The command first restores default mapping for both EBCDIC and ASCII characters. In the **no** form of the command, the **all** keyword resets all character mappings to Cisco defaults.

Table 128 shows the default character mappings between ASCII and EBCDIC in decimal and hexadecimal format.

To convert outgoing ASCII characters into EBCDIC characters, use the **keymap** command to modify the keymap structure with the tag *ebcdic_xx=string*, where *xx* is a hexadecimal value and *string* is the sequence of characters that send the EBCDIC character.

Table 135 Default ASCII, EBCDIC Character Mappings

Character	ASCII Decimal	ASCII Hexadecimal	EBCDIC Decimal	EBCDIC Hexadecimal
!	33	0x21	90	0x5a
"	34	0x22	127	0x7f
#	35	0x23	123	0x7b
\$	36	0x24	91	0x5b
%	37	0x25	108	0x6c
&	38	0x26	80	0x50
'	39	0x27	125	0x7d
(40	0x28	77	0x4d
)	41	0x29	93	0x5d
*	42	0x2a	92	0x5c
+	43	0x2b	78	0x4e
,	44	0x2c	107	0x6b
-	45	0x2d	96	0x60
.	46	0x2e	75	0x4b
/	47	0x2f	97	0x61
0	48	0x30	240	0xf0
1	49	0x31	241	0xf1
2	50	0x32	242	0xf2
3	51	0x33	243	0xf3
4	52	0x34	244	0xf4
5	53	0x35	245	0xf5
6	54	0x36	246	0xf6
7	55	0x37	247	0xf7
8	56	0x38	248	0xf8
9	57	0x39	249	0xf9
:	58	0x3a	122	0x7a
;	59	0x3b	94	0x5e
<	60	0x3c	76	0x4c
=	61	0x3d	126	0x7e
>	62	0x3e	110	0x6e
?	63	0x3f	111	0x6f
@	64	0x40	124	0x7c
A	65	0x41	193	0xc1
B	66	0x42	194	0xc2
C	67	0x43	195	0xc3
D	68	0x44	196	0xc4

Table 135 Default ASCII, EBCDIC Character Mappings (continued)

Character	ASCII Decimal	ASCII Hexadecimal	EBCDIC Decimal	EBCDIC Hexadecimal
E	69	0x45	197	0xc5
F	70	0x46	198	0xc6
G	71	0x47	199	0xc7
H	72	0x48	200	0xc8
I	73	0x49	201	0xc9
J	74	0x4a	209	0xd1
K	75	0x4b	210	0xd2
L	76	0x4c	211	0xd3
M	77	0x4d	212	0xd4
N	78	0x4e	213	0xd5
O	79	0x4f	214	0xd6
P	80	0x50	215	0xd7
Q	81	0x51	216	0xd8
R	82	0x52	217	0xd9
S	83	0x53	226	0xe2
T	84	0x54	227	0xe3
U	85	0x55	228	0xe4
V	86	0x56	229	0xe5
W	87	0x57	230	0xe6
X	88	0x58	231	0xe7
Y	89	0x59	232	0xe8
Z	90	0x5a	233	0xe9
[91	0x5b	173	0xad
\	92	0x5c	224	0xe0
]	93	0x5d	189	0xbd
^	94	0x5e	95	0x5f
_	95	0x5f	109	0x6d
`	96	0x60	121	0x79
a	97	0x61	129	0x81
b	98	0x62	130	0x82
c	99	0x63	131	0x83
d	100	0x64	132	0x84
e	101	0x65	133	0x85
f	102	0x66	134	0x86
g	103	0x67	135	0x87
h	104	0x68	136	0x88

Table 135 Default ASCII, EBCDIC Character Mappings (continued)

Character	ASCII Decimal	ASCII Hexadecimal	EBCDIC Decimal	EBCDIC Hexadecimal
i	105	0x69	137	0x89
j	106	0x6a	145	0x91
k	107	0x6b	146	0x92
l	108	0x6c	147	0x93
m	109	0x6d	148	0x94
n	110	0x6e	149	0x95
o	111	0x6f	150	0x96
p	112	0x70	151	0x97
q	113	0x71	152	0x98
r	114	0x72	153	0x99
s	115	0x73	162	0xa2
t	116	0x74	163	0xa3
u	117	0x75	164	0xa4
v	118	0x76	165	0xa5
w	119	0x77	166	0xa6
x	120	0x78	167	0xa7
y	121	0x79	168	0xa8
z	122	0x7a	169	0xa9
{	123	0x7b	192	0xc0
	124	0x7c	79	0x4f
}	125	0x7d	208	0xd0
~	126	0x7e	161	0xa1

Examples

The following example creates a two-way binding between an EBCDIC character and an ASCII character:

```
tn3270 character-map 0x81 0x78
```

Related Commands

Command	Description
show tn3270 ascii-hexval	Displays ASCII-hexadecimal character mappings.
show tn3270 character-map	Displays character mappings between ASCII and EBCDIC.

tn3270 datastream

To enable the TN3270 extended datastream, use the **tn3270 datastream** command in global configuration mode. Use the **no** form of this command to return to the normal TN3270 datastream.

tn3270 datastream {extended | normal}

no tn3270 datastream

Syntax Description	extended	Extended datastream.
	normal	Normal datastream.

Defaults Normal datastream

Command Modes Global configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines This command causes an “-E” to be appended to the terminal type string sent to the IBM host. This allows you to use the extended TN3270 features.

Examples The following example shows the supported tn3270 datastream options:

```
# tn3270 datastream ?
  extended  Use extended TN3270 datastream
  normal    Use normal TN3270 datastream
```

tn3270 null-processing

To specify how NULLs are handled, use the **tn3270 null-processing** command in global configuration mode. Use the **no** form of the command to return to 7171 NULL processing.

tn3270 null-processing [**3270** | **7171**]

no tn3270 null-processing [**3270** | **7171**]

Syntax Description

3270	(Optional) NULLs are compressed out of the string, as on a 3278-x terminal.
7171	(Optional) NULLs are converted to spaces, as on a 7171 controller.

Defaults

7171 NULL processing

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

If a user enters data, uses an arrow key to move the cursor to the right on the screen, and then enters more data, the intervening spaces are filled with NULLs. To specify how NULLs are handled, enter the **tn3270 null-processing** command either with the **3270** argument, where NULLs are compressed out of the string (as on a real 3278-x terminal) or the argument **7171**, where NULLs are converted to spaces as on a 7171 controller. Enter this command in global configuration.

Examples

This example shows the two available null processing methods:

```
tn3270 null-processing ?
 3270 Use 3270-style null processing
 7171 Use 7171-style null processing
```

tn3270 optimize-cursor-move

To increase performance between a remote user and a TN3270 host by limiting cursor movement information that is sent to user terminals, issue the **tn3270 optimize-cursor-move** command in global configuration mode. Use the **no** form of the command to ensure that all cursor movement information is sent between the user's terminal and the TN3270 host.

tn3270 optimize-cursor-move

no tn3270 optimize-cursor-move

Syntax Description This command has no arguments or keywords.

Defaults Cursor movement escape strings are sent to the terminal.

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines Issuing this command increases the speed of information transfer between users and TN3270 hosts through an access server.

If you do not issue this command, virtually every byte of information between the user's terminal and the TN3270 host is prepended and trailed by cursor-movement strings.

Examples The following example disables status messages to users who are connected to 3278 terminals:

```
tn3270 optimize-cursor-move
```

Related Commands	Command	Description
	tn3270 status-message	Reenables the display of status messages after they have been disabled.

tn3270 reset-required

To lock a terminal after input error until the user resets the terminal, use the **tn3270 reset-required** command in global configuration mode. Use the **no** form of the command to return to the default of no reset required.

tn3270 reset-required

no tn3270 reset-required

Syntax Description This command has no arguments or keywords.

Defaults No reset is required

Command Modes Global configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines On a 3278-x terminal, the keyboard is locked and further input is not permitted after input error (due to field overflow, invalid entry, and so on), until the user presses the RESET key. Most TN3270 implementations leave the keyboard unlocked and remove any error message on the next key input after the error. Use this command to lock the keyboard until the user performs a reset.

tn3270 status-message

To reenble the display of status messages after they have been disabled, use the **tn3270 status-message** command in global configuration mode. Use the **no** form of this command to save bandwidth on asynchronous lines by not displaying status messages.

tn3270 status-message

no tn3270 status-message

Syntax Description This command has no arguments or keywords.

Defaults Status messages appear.

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines Status messages appear on the user's console by default. These messages include "System Locked," "Field error," and "System UnLocked" messages, among others. These messages are sent back to the user's terminal via the TTY line on the access server.

Disabling status messages saves bandwidth on asynchronous lines, which have very low bandwidth.

Examples The following example disables status messages to users who are connected to 3270 terminals:

```
no tn3270 status-message
```

Related Commands	Command	Description
	tn3270 optimize-cursor-move	Increases performance between a remote user and a TN3270 host by limiting cursor movement information that is sent to user terminals.

tn3270 typeahead

To buffer keyboard data when a 3278 server is in locked mode, use the **tn3270 typeahead** command in global configuration mode. Use the **no** form of this command to disable the typeahead function.

tn3270 typeahead

no tn3270 typeahead

Syntax Description This command has no arguments or keywords.

Defaults No typeahead

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines When typeahead is enabled, the TN3270 client implementation in the Cisco IOS software permits you (the user) to continue typing while the system is trying to obtain a response from the TN3270 server. Information you type while a “System Locked” message appears on the terminal is stored in a buffer. After the “System Locked” message disappears, the information is then used as though it were just typed.

Examples The following example saves user information when “System Locked” messages appear on the screen:

```
tn3270 typeahead
```

Related Commands	Command	Description
	tn3270 reset-required	Locks a terminal after input error until the user resets the terminal.
