

Configuring Terminal Operating Characteristics for Dial-In Sessions

This chapter describes how to set operating characteristics for remote terminal service connections. In line configuration mode, you can set terminal operating characteristics that will be in operation for that line until the next time you change the line parameters. Alternatively, you can change the line setting temporarily with the **terminal EXEC** commands as described later in this chapter.

First, select a preferred connection protocol then configure the appropriate communication parameters:

- Select a Connection Protocol
- Configure Communication Parameters for Terminal Ports

For a complete description of the terminal characteristic commands in this chapter, refer to the *Dial Solutions Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Select a Connection Protocol

The preferred transport type is your preferred connection protocol. This section describes how to configure the router to support specific protocols for connection sessions over a line.

- All Sessions on a Line
- Individual Sessions

All Sessions on a Line

Use the **transport preferred** command to specify which transport protocol is used on connections. Use the **transport input** and **transport output** commands to explicitly specify the protocols allowed on individual lines for both incoming and outgoing connections.

Note Cisco routers do not accept incoming network connections to asynchronous ports (TTY lines) by default. You have to specify an incoming transport protocol, or specify **transport input all** before the line will accept incoming connections. For example, if you are using your router as a terminal server to make console-port connections to routers or other devices, you will not be able to use Telnet to connect to these devices. You will receive the message “Connection Refused.”

For routers that support LAT, the default protocol for outgoing connections is LAT. For those that do not support LAT, the default protocol for outgoing connections is Telnet. For incoming connections, all the supported network protocols are accepted (the default protocol is **all**).

Use the following commands in line configuration mode to specify transport protocols:

Command	Purpose
transport input {all lat mop nasi none pad rlogin ssh telnet v120}	Define which protocols can be used to connect to a specific line.
transport output {all lat mop nasi none pad rlogin telnet v120}	Determine the protocols that can be used for outgoing connections from a line.
transport preferred {all lat mop nasi pad rlogin telnet v120}	Specify the protocol for the router to use if the user did not specify a protocol.
transport preferred none	Prevent errant connection attempts.

The router accepts a host name entry at the EXEC system prompt as a Telnet command. If you enter the host name incorrectly, the router interprets the entry as an incorrect Telnet command and provides an error message indicating that the host does not exist. The **transport preferred none** command disables this option so that if you enter a command incorrectly at the EXEC prompt, the router does not attempt to make a Telnet connection to a host that it cannot find.

The **transport preferred** setting specifies a search order when attempting to resolve names that might be valid for multiple protocols. If the address or service does not match the preferred protocol, all other valid output protocols are searched to find a valid match.

Individual Sessions

You can configure the Cisco IOS software to save local parameters between sessions. These local parameters are set with the EXEC **terminal** commands.

To specify the preferred protocol to use for the current session when a command does not specify one, use the following command in EXEC mode:

Command	Purpose
terminal transport preferred {all lat mop nasi none pad rlogin telnet v120}	Specify the protocol for the Cisco IOS software to use for the current session if the user did not specify a protocol.

The preferred transport type is your preferred connection protocol. This setting specifies a protocol search order that the Cisco IOS software uses when it attempts to resolve a device name that you enter, but you do not specify a connection protocol. For example, if you want to connect to a TCP/IP host named host1 and want to use Telnet, you type **telnet host1**. However, if your preferred connection protocol is set to Telnet, you could type **host1** and be connected to the device. A host name might be valid for multiple protocols. If the address or service does not match the preferred protocol, all other valid connection protocols are searched to find a valid match for the name.

For router software images that support LAT, the default protocol for outgoing connections is LAT. For router software images that do not support LAT, the default protocol for outgoing connections is Telnet. For incoming connections, all the supported network protocols are accepted (the default protocol is **all**).

The Cisco IOS software accepts a host name entry at the EXEC prompt as a Telnet command. If you enter the host name incorrectly, the Cisco IOS software interprets the entry as an incorrect Telnet command and provides an error message indicating that the host does not exist. The **transport preferred none** command disables this option so that if you enter a command incorrectly at the EXEC prompt, the Cisco IOS software does not attempt to make a Telnet connection.

Configure Communication Parameters for Terminal Ports

The following communication parameters can be configured:

- Configure All Sessions on a Line
- Configure Individual Sessions
- Change the Default Privilege Level for Lines
- Enable Password Checking at Login
- Display Line Connection Information after the Login Prompt
- Establish Terminal Session Limits

Configure All Sessions on a Line

The Cisco IOS software supplies the following default serial communication parameters for terminal and other serial device operation:

- 9600 bits per second (bps) line speed
- 8 data bits
- 2 stop bits
- No parity bit

You can change these parameters as necessary to meet the requirements of the terminal or host to which you are connected. To do so, use the following commands in line configuration mode:

Command	Purpose
speed <i>bps</i> txspeed <i>bps</i> rxspeed <i>bps</i>	Set the line speed. Choose from line speed, transmit speed, or receive speed.
databits {5 6 7 8}	Set the data bits.
stopbits {1 1.5 2}	Set the stop bits.
parity {none even odd space mark}	Set the parity bit.

Configure Individual Sessions

You can change these parameters as necessary to meet the requirements of the terminal or host to which you are attached. To do so, use the following commands in EXEC mode:

Command	Purpose
terminal speed <i>bps</i> terminal txspeed <i>bps</i> terminal rxspeed <i>bps</i>	Set the line speed for the current session. Choose from line speed, transmit speed, or receive speed.
terminal databits {5 6 7 8}	Set the data bits for the current session.
terminal stopbits {1 1.5 2}	Set the stop bits for the current session.
terminal parity {none even odd space mark}	Set the parity bit for the current session.

Change the Default Privilege Level for Lines

To change the default privilege level for a given line or a group of lines, use the following command in line configuration mode:

Command	Purpose
<code>privilege level level</code>	Specify a default privilege level for a line.

Enable Password Checking at Login

You can enable password checking on a particular line so that the user is prompted to enter a password at the system login screen. You must then also specify a password. To do so, use the following commands in line configuration mode:

Step	Command	Purpose
1	<code>login</code>	Enable password checking on a per-line basis using the password specified with the <code>password</code> command.
2	<code>password password</code>	Assign a password to a particular line.

You can enable password checking on a per-user basis, in which case authentication is based on the username specified with the `username` global configuration command. To enable password checking on a per-user basis, use the following commands in line configuration mode:

Step	Command	Purpose
1	<code>login local</code>	Enable password checking on a per-user basis using the username and password specified with the <code>username</code> global configuration command.
2	<code>login tacacs</code> or <code>login authentication { default list-name }</code>	Select the TACACS-style user ID and password-checking mechanism.

Use the `login tacacs` command with Terminal Access Controller Access Control System (TACACS) and Extended TACACS. Use the `login authentication` command with AAA/TACACS+.

By default, virtual terminals require passwords. If you do not set a password for a virtual terminal, the router displays an error message and closes the attempted connection. Use the `no login` command to disable this function and allow connections without a password.

For other access control tasks and password restrictions, including the `enable password` global configuration command that restricts access to privileged mode, see the *Security Configuration Guide*.

Establish Terminal Session Limits

You might need to control terminal sessions in high-traffic areas to provide resources for all users. You can define the following limitations for terminal sessions:

- The maximum number of sessions
- The idle session timeout interval or the absolute timeout interval

To establish terminal session limits, use the following commands in line configuration mode:

Command	Purpose
session-limit <i>session-number</i> ¹	Set the maximum number of simultaneous sessions.
session-timeout <i>minutes</i> [output]	Set the idle session timeout interval.
or	or
absolute-timeout <i>minutes</i>	Set the absolute timeout interval.
logout-warning [<i>seconds</i>]	Warn users of impending timeouts set with the absolute-timeout command.

1 There is no inherent upper limit to the number of sessions you can create.

Note The **absolute-timeout** command overrides any timeouts set through the AppleTalk Remote Access (ARA) protocol.

Display Line Connection Information after the Login Prompt

You can display the host name, line number, and location of the host each time an EXEC session is started or an incoming connection is made. The line number banner appears immediately after the EXEC banner or incoming banner. This feature is useful for tracking problems with modems because it lists the host and line for the modem connection. Modem type information is also included if applicable.

To provide line information, use the following command in global configuration mode:

Command	Purpose
service linenum	Provide service line-number information after the EXEC banner or incoming banner.

