

Using the Command-Line Interface

The Cisco IOS command-line interface (CLI) is the primary user interface used for configuring, monitoring, and maintaining Cisco devices. This user interface provides direct and simple execution of Cisco Internetwork Operating System (IOS) commands, whether using a router console or terminal, or using remote access methods.

This chapter describes the basic features of the Cisco IOS command-line interface and how to use them. Topics covered include navigation and editing features, help features, command history features, and Cisco IOS command modes.

Additional user interfaces include the Cisco Web Browser, and user-menus configured by a system administrator. For information on issuing commands using the Cisco Web Browser, see the “Using the Cisco Web Browser” chapter of this book. For information on user-menus, see the “Managing Connections, Menus, and System Banners” chapter of this book.

For a complete description of the user interface commands in this chapter, refer to the “Basic Command-Line Interface Commands” chapter of the *Configuration Fundamentals Command Reference*. To locate documentation of other commands, use the command reference index or search online.

This chapter contains information about the following command-line interface topics:

- Understanding Cisco IOS Command Modes
- Using the No and Default Forms of Commands
- Getting Context-Sensitive Help
- Checking Command Syntax
- Using the Command History Features
- Using the Editing Features

As a further context for understand Cisco IOS Command Modes, this chapter also contains:

- Summary of Cisco IOS Configuration Modes

Understanding Cisco IOS Command Modes

The Cisco IOS command-line interface is divided into many different modes. The commands available to you at any given time depend on which mode you are currently in. Entering a question mark (?) at the system prompt allows you to obtain a list of commands available for each command mode.

For security purposes, Cisco routers have two basic levels of access to commands: *user EXEC mode* and *privileged EXEC mode*.

When you start a session on the router, you begin in *user EXEC mode*. Only a limited subset of EXEC commands are available in user EXEC mode. This level of access is reserved for non-configuration tasks like checking the router status.

In order to have access to all commands, you must enter *privileged EXEC mode*. Normally, you must enter a password to enter privileged EXEC mode. From privileged mode, you can enter any EXEC command or enter *global configuration mode*. Most of the EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The EXEC commands are not saved across reboots of the router.

Configuration modes allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across router reboots. In order to access the various configuration modes, you must start at *global configuration mode*. From global configuration mode, you can enter *interface configuration mode*, *subinterface configuration mode*, and a variety of protocol-specific modes.

ROM monitor mode is a separate mode used when the router cannot boot properly. If your router or access server does not find a valid system image when it is booting, or if its configuration file is corrupted at startup, the system might enter read-only memory (ROM) monitor mode.

The following sections describe how to access the main Cisco IOS command modes:

- User EXEC Mode
- Privileged EXEC Mode
- Global Configuration Mode
- Interface Configuration Mode
- Subinterface Configuration Mode
- ROM Monitor Mode

These sections are followed by a table (Table 42) summarizing the main command modes, showing prompt examples and access/exit methods. For a summary of all the Cisco IOS command modes, see the final section of this chapter,

User EXEC Mode

After you log in to the router or access server, you are automatically in user EXEC command mode. The EXEC commands available at the user level are a subset of those available at the privileged level. In general, the user EXEC commands allow you to connect to remote devices, change terminal settings on a temporary basis, perform basic tests, and list system information.

To list the user EXEC commands, use the following command:

Command	Purpose
?	Lists the user EXEC commands.

The user-level prompt consists of the host name followed by the angle bracket (>):

```
Router>
```

The default host name is `Router` unless it has been changed during initial configuration using the **setup** command. Refer to the product user guide for information on the **setup** facility. You can also change the host name using the **hostname** global configuration command described in the “Basic System Management Commands” chapter in the *Configuration Fundamentals Command Reference*.

To list the commands available in user EXEC mode, enter a question mark (?) as shown in the following example:

```
Router> ?
Exec commands:
<1-99>          Session number to resume
connect         Open a terminal connection
disconnect      Disconnect an existing telnet session
enable          Turn on privileged commands
exit           Exit from the EXEC
help           Description of the interactive help system
lat            Open a lat connection
lock           Lock the terminal
login          Log in as a particular user
logout         Exit from the EXEC
menu           Start a menu-based user interface
mbranch        Trace multicast route for branch of tree
mrbranch       Trace reverse multicast route to branch of tree
mtrace         Trace multicast route to group
name-connection Name an existing telnet connection
pad            Open a X.29 PAD connection
ping           Send echo messages
resume         Resume an active telnet connection
show           Show running system information
systat         Display information about terminal lines
telnet         Open a telnet connection
terminal       Set terminal line parameters
tn3270         Open a tn3270 connection
trace          Trace route to destination
where          List active telnet connections
x3            Set X.3 parameters on PAD
xremote        Enter XRemote mode
```

The list of commands might vary slightly from this example, depending on the software feature set and configuration of the product.

Privileged EXEC Mode

Because many of the privileged commands set operating parameters, privileged access should be password protected to prevent unauthorized use. The privileged command set includes those commands contained in user EXEC mode, as well as the **configure** command through which you can access the remaining command modes. Privileged EXEC mode also includes high-level testing commands, such as **debug**. For details on the **debug** commands, see the *Debug Command Reference*.

The privileged EXEC mode prompt consists of the device's host name followed by the pound sign (#). (If the router or access server was named with the **hostname** command, that name would appear as the prompt instead of "Router.")

```
Router#
```

To access and list the privileged EXEC commands, use the following commands:

Step	Command	Purpose
1	enable [<i>password</i>]	Enters the privileged EXEC mode.
2	?	Lists privileged EXEC commands.

If the system administrator has set a password, you are prompted to enter it before being allowed access to privileged EXEC mode. The password is not displayed on the screen and is case sensitive. If an enable password has not been set, enable mode can be accessed only from the router console.

The system administrator uses the **enable password** global configuration command to set the password that restricts access to privileged mode. This command is described in the “Passwords and Privileges Commands” chapter in the *Security Command Reference*.

The following example shows how to access privileged EXEC mode:

```
Router> enable
Password:letmein
Router#
```

To return from privileged EXEC mode to user EXEC mode, use the following command:

Command	Purpose
disable	Moves from privileged EXEC mode to user EXEC mode.

From the privileged level, you can access global configuration mode. For instructions, see the “Global Configuration Mode” section, which follows this section.

Global Configuration Mode

Global configuration commands apply to features that affect the system as a whole, rather than just one protocol or interface. From global configuration mode you can also enter specific configuration modes and submodes used to configure specific system features. Use the **configure terminal** privileged EXEC command to enter global configuration mode.

Commands to enable a particular routing or bridging function are also global configuration commands. For information on protocol-specific global configuration commands, see the appropriate configuration guide in the Cisco IOS software documentation.

To access and list the global configuration commands, use the following commands:

Step	Command	Purpose
1	configure terminal	At the terminal, from the privileged EXEC mode, enters global configuration mode.
2	?	Lists the global configuration commands.

The following example shows the process of entering global configuration mode from privileged EXEC mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Note that the system prompt changes to indicate that you are now in global configuration mode. The prompt for global configuration mode consists of the host-name of the device followed by `(config)` and the pound sign (`#`). To list the commands available in privileged EXEC mode, issue the `?` command at the prompt.

Commands entered in global configuration mode update the running configuration file as soon as they are entered. In other words, changes to the configuration take effect each time you press the Enter or Return key at the end of a valid command. However, these changes are not saved into the startup configuration file until you issue the **copy running-config startup-config** EXEC mode command. This behavior is explained in more detail later in this document.

As shown in the example above, the system dialogue prompts you to end your configuration session (exit configuration mode) by pressing the Control (Ctrl) and “z” keys simultaneously; when you press these keys, **^Z** is printed to the screen. You can actually end your configuration session by

entering the Ctrl-Z key combination, using the **end** command, using the Ctrl-C key combination. The **end** command is the recommended way to indicate to the system that you are done with the current configuration session.

Note If you use Ctrl-Z at the end of a command line in which a valid command has been typed, that command will be added to the running configuration file. In other words, using Ctrl-Z is equivalent to hitting the Enter (Carriage Return) key before exiting. For this reason, it is safer to end your configuration session using the end command. Alternatively, you can use the Ctrl-C key combination to end your configuration session without sending a Carriage Return signal.

You can also use the **exit** command to return from global configuration mode to EXEC mode, but this only works in global configuration mode. Pressing Ctrl-Z or entering the **end** command will always take you back to EXEC mode regardless of which configuration mode or configuration submode you are in.

To exit global configuration command mode and return to privileged EXEC mode, use one of the following commands: To exit global configuration command mode and return to privileged EXEC mode, use one of the following commands:

Command	Purpose
end or ^Z	Ends the current configuration session and returns to privileged EXEC mode.
exit	Exits the current command mode and returns to the preceding mode. For example, exits from global configuration mode to privileged EXEC mode.

From global configuration mode, you can access a number of other command modes. These command modes are described in the sections that follow. For a complete list of these modes, see the section “Other Configuration Modes.”

Interface Configuration Mode

Many features are enabled on a per-interface basis. Interface configuration commands modify the operation of an interface such as an Ethernet, FDDI, or serial port. Interface configuration commands always follow an **interface** global configuration command, which defines the interface type.

For details on interface configuration commands that affect general interface parameters, such as bandwidth, clock rate, and so on, see the “Interface Commands” chapter in the *Configuration Fundamentals Command Reference*. For protocol-specific commands, see the appropriate Cisco IOS software command reference.

To access and list the interface configuration commands, use the following commands:

Step	Command	Purpose
1	interface <i>type number</i>	From global configuration mode, enters interface configuration mode.
2	?	Lists the interface configuration commands.

In the following example, serial interface 0 is about to be configured. The new prompt Router (config-if) # indicates interface configuration mode.

```
Router(config)# interface serial 0 <Return>
Router(config-if)#
```

To exit interface configuration mode and return to global configuration mode, enter the **exit** command. To exit configuration mode and return to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.

Subinterface Configuration Mode

You can configure multiple virtual interfaces (called subinterfaces) on a single physical interface. Subinterfaces appear to be distinct physical interfaces to the various protocols. For example, Frame Relay networks provide multiple point-to-point links called permanent virtual circuits (PVCs). PVCs can be grouped under separate subinterfaces that in turn are configured on a single physical interface. From a bridging spanning-tree viewpoint, each subinterface is a separate bridge port, and a frame arriving on one subinterface can be sent out on a another subinterface.

Subinterfaces also allow multiple encapsulations for a protocol on a single interface. For example, a router or access server can receive an ARPA-framed IPX packet and forward the packet back out the same physical interface as a SNAP-framed IPX packet.

For detailed information on how to configure subinterfaces, see the appropriate module for a specific protocol in the Cisco IOS software documentation.

To access and list the subinterface configuration commands, use the following commands:

Step	Command	Purpose
1	See the example that follows. For information on interface commands that allow subinterface implementation, see the protocol specific chapter later in this publication.	From interface configuration mode, configures a virtual interface.
2	?	Lists the subinterface configuration commands.

In the following example, a subinterface is configured for serial line 2, which is configured for Frame Relay encapsulation. The subinterface is called 2.1 to indicate that it is subinterface 1 of serial interface 2. The new prompt `Router(config-subif)#` indicates that you are in subinterface configuration mode. The subinterface can be configured to support one or more Frame Relay PVCs.

```
Router(config)# interface serial 2
Router(config-if)# encapsulation frame-relay
Router(config-if)# interface serial 2.1
Router(config-subif)#
```

To exit subinterface configuration mode and return to global configuration mode, enter the **exit** command. To exit configuration mode and return to privileged EXEC mode, press **Ctrl-Z**.

ROM Monitor Mode

If your router or access server does not find a valid system image, or if you interrupt the boot sequence, the system might enter read-only memory (ROM) monitor mode. From ROM monitor mode, you can boot the device or perform diagnostic tests.

You can also enter ROM monitor mode by entering the **reload** EXEC command and then pressing the Break key during the first 60 seconds of startup. If you have changed the configuration, use the **copy running-config startup-config** command and then issue the **reload** command to save your configuration changes.

To access and list the ROM monitor configuration commands, use the following commands:

Step	Command	Purpose
1	reload Press the Break key during the first 60 seconds while the system is booting.	Enters ROM monitor mode from privileged EXEC mode.
2	?	Lists the ROM monitor commands.

The ROM monitor prompt is the angle bracket (>):

```
> ?
$ state      Toggle cache state (? for help)
B [filename] [TFTP Server IP address | TFTP Server Name]
              Load and execute system image from ROM or from TFTP server
C [address]  Continue execution [optional address]
D /S M L V   Deposit value V of size S into location L with modifier M
E /S M L     Examine location L with size S with modifier M
G [address]  Begin execution
H           Help for commands
I           Initialize
K           Stack trace
L [filename] [TFTP Server IP address | TFTP Server Name]
              Load system image from ROM or from TFTP server, but do not
              begin execution
O           Show configuration register option settings
P           Set the break point
S           Single step next instruction
T function   Test device (? for help)
Deposit and Examine sizes may be B (byte), L (long) or S (short).
Modifiers may be R (register) or S (byte swap).
Register names are: D0-D7, A0-A6, SS, US, SR, and PC
```

To return to user EXEC mode, type **continue**. To initialize the router or access server, enter the **i** command. The **i** command causes the bootstrap program to reinitialize the hardware, clear the contents of memory, and boot the system. (It is best to issue the **i** command before you run any tests or boot software.) To boot the system image file, use the **b** command (see the “Rebooting a Router” chapter). For details on ROM monitor mode commands, refer to the appropriate hardware installation guide.

Summary of the Main Cisco IOS Command Modes

Table 42 summarizes the main command modes of the Cisco IOS software.

Table 42 Summary of the Main Cisco IOS Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	Router>	Use the logout command.
Privileged EXEC	From user EXEC mode, use the enable EXEC command.	Router#	To exit back to user EXEC mode, use the disable command. To enter global configuration mode, use the configure terminal privileged EXEC command.
Global configuration	From privileged EXEC mode, use the configure terminal privileged EXEC command.	Router(config)#	To exit to privileged EXEC mode, use the exit or end command or press Ctrl-Z . To enter interface configuration mode, use the interface configuration command.
Interface configuration	From global configuration mode, enter by specifying an interface with an interface command.	Router(config-if)#	To exit to global configuration mode, use the exit command. To exit to privileged EXEC mode, use the exit command or press Ctrl-Z . To enter subinterface configuration mode, specify a subinterface with the interface command.
Subinterface configuration	From interface configuration mode, specify a subinterface with an interface command.	Router(config-subif)#	To exit to global configuration mode, use the exit command. To enter privileged EXEC mode, use the end command or press Ctrl-Z .
ROM monitor	From privileged EXEC mode, use the reload EXEC command. Press the Break key during the first 60 seconds while the system is booting.	>	To exit to user EXEC mode, use the continue command.

Getting Context-Sensitive Help

Entering a question mark (?) at the system prompt displays a list of commands available for each command mode. You can also get a list of any command's associated keywords and arguments with the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, perform one of the following commands:

Step	Command	Purpose
1	help	Obtain a brief description of the help system in any command mode.
2	<i>abbreviated-command-entry?</i>	Obtain a list of commands that begin with a particular character string.
3	<i>abbreviated-command-entry</i> <Tab>	Complete a partial command name.
4	?	List all commands available for a particular command mode.
5	<i>command ?</i>	List a command's associated keywords.
6	<i>command keyword ?</i>	List a keyword's associated arguments.

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?). Do not include a space. This form of help is called *word help*, because it completes a word for you.

To list keywords or arguments, enter a question mark (?) in place of a keyword or argument. Include a space before the ?. This form of help is called *command syntax help*, because it reminds you which keywords or arguments are applicable based on the command, keywords, and arguments you already have entered.

You can abbreviate commands and keywords to the number of characters that allow a unique abbreviation. For example, you can abbreviate the **show** command to **sh**.

Enter the **help** command (which is available in any command mode) for a brief description of the help system:

```
Router# help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must back up until entering a '?' shows the
available options.
Two styles of help are provided:
 1. Full help is available when you are ready to enter a
    command argument (e.g. 'show ?') and describes each possible
    argument.
 2. Partial help is provided when an abbreviated argument is entered
    and you want to know what arguments match the input
    (e.g. 'show pr?'.)
```

As described in the **help** command output, you can enter a partial command name and a question mark (?) to obtain a list of commands beginning with a particular character set. (See the section "Complete a Partial Command Name" later in this chapter for more details.)

Example of Context Sensitive Help

The following example illustrates how the context-sensitive help feature enables you to create an access list from configuration mode.

Enter the letters **co** at the system prompt followed by a question mark (?). Do not leave a space between the last letter and the question mark (?). The system provides the commands that begin with **co**.

```
Router# co?  
configure connect copy
```

Enter the **configure** command followed by a space and a question mark (?) to list the command's keywords and a brief explanation:

```
Router# configure ?  
memory      Configure from NV memory  
network     Configure from a TFTP network host  
terminal    Configure from the terminal  
<cr>
```

Enter the **terminal** keyword to enter configuration mode from the terminal:

```
Router# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#
```

Enter the **access-list** command followed by a space and a question mark (?) to list the command's keywords:

```
Router(config)# access-list ?  
<1-99>      IP standard access list  
<100-199>   IP extended access list  
<1000-1099> IPX SAP access list  
<1100-1199> Extended 48-bit MAC address access list  
<200-299>   Protocol type-code access list  
<300-399>   DECnet access list  
<400-499>   XNS standard access list  
<500-599>   XNS extended access list  
<600-699>   Appletalk access list  
<700-799>   48-bit MAC address access list  
<800-899>   IPX standard access list  
<900-999>   IPX extended access list
```

The two numbers within the angle brackets represent an inclusive range. Enter the access list number **99** and then enter another question mark (?) to see the arguments that apply to the keyword and brief explanations:

```
Router(config)# access-list 99 ?  
deny       Specify packets to reject  
permit     Specify packets to forward
```

Enter the **deny** argument followed by a question mark (?) to list additional options:

```
Router(config)# access-list 99 deny ?  
A.B.C.D    Address to match
```

Generally, uppercase letters represent variables, though this is not always the case. Enter the IP address followed by a question mark (?) to list additional options:

```
Router(config)# access-list 99 deny 131.108.134.0 ?  
A.B.C.D    Mask of bits to ignore  
<cr>
```

The `<cr>` symbol appears in the list to indicate that one of your options is to press Return to execute the command.

The other option is to add a wildcard mask. Enter the wildcard mask followed by a question mark (?) to list further options.

```
Router(config)# access-list 99 deny 131.108.134.0 0.0.0.255 ?
<cr>

Router(config)# access-list 99 deny 131.108.134.0 0.0.0.255
```

The `<cr>` symbol by itself indicates there are no more keywords or arguments. Press Return to execute the command. The system adds an entry to access list 99 that denies access to all hosts on subnet 131.108.134.0.

Display Help for All User-Level Commands

To configure a line to display help for the full set of user-level commands during all sessions, use the following commands in line configuration mode:

Command	Purpose
full-help	Configure a line or lines to receive help for the full set of user-level commands when a user presses ?.

To configure the current session to display help for the full set of user-level commands, use the following command in user **exec** mode:

Command	Purpose
terminal full-help	Configure this session to provide help for the full set of user-level commands.

The **full-help** and **terminal full-help** commands enable (or disable) a display of all help messages available from the terminal. They are used with the **show** command.

The following example is output for **show ?** with **terminal full-help** disabled and then enabled:

```
Router> show ?
 bootflash  Boot Flash information
 calendar   Display the hardware calendar
 clock      Display the system clock
 context    Show context information
 dialer     Dialer parameters and statistics
 history    Display the session command history
 hosts      IP domain-name, lookup style, nameservers, and host table
 isdn       ISDN information
 kerberos   Show Kerberos Values
 modemcap   Show Modem Capabilities database
 ppp        PPP parameters and statistics
 rmon       rmon statistics
 sessions   Information about Telnet connections
 snmp       snmp statistics
 terminal    Display terminal configuration parameters
 users      Display information about terminal lines
 version    System hardware and software status

Router> terminal full-help
Router> show ?
 access-expression  List access expression
 access-lists       List access lists
```

aliases	Display alias commands
apollo	Apollo network information
appletalk	AppleTalk information
arp	ARP table
async	Information on terminal lines used as router interfaces
bootflash	Boot Flash information
bridge	Bridge Forwarding/Filtering Database [verbose]
bsc	BSC interface information
bstun	BSTUN interface information
buffers	Buffer pool statistics
calendar	Display the hardware calendar
cdp	CDP information
clns	CLNS network information
clock	Display the system clock
cls	DLC user information
cmns	Connection-Mode networking services (CMNS) information
...	
x25	X.25 information
xns	XNS information
xremote	XRemote statistics

Checking Command Syntax

The user interface provides error isolation in the form of an error indicator, a caret symbol (^). The ^ symbol appears at the point in the command string where you have entered an incorrect command, keyword, or argument.

In the following example, suppose you want to set the clock. Use context-sensitive help to check the syntax for setting the clock.

```
Router# clock ?
      set Set the time and date
Router# clock
```

The help output shows that the **set** keyword is required. Check the syntax for entering the time:

```
Router# clock set ?
hh:mm:ss Current time
Router# clock set
```

Enter the current time:

```
Router# clock set 13:32:00
% Incomplete command.
```

The system indicates that you need to provide additional arguments to complete the command. Press **Ctrl-P** (see the next section, “Use the Command History Features”) to automatically repeat the previous command entry. Then add a space and question mark (?) to reveal the additional arguments:

```
Router# clock set 13:32:00 ?
<1-31> Day of the month
January Month of the year
February
March
April
May
June
July
August
September
October
November
December
```

Now you can complete the command entry:

```
Router# clock set 13:32:00 23 February 97
                                     ^
% Invalid input detected at '^' marker.
```

The caret symbol (^) and help response indicate an error at 97. To list the correct syntax, enter the command up to the point where the error occurred and then enter a question mark (?):

```
Router# clock set 13:32:00 23 February ?
<1993-2035> Year
Router# clock set 13:32:00 23 February
```

Enter the year using the correct syntax and press Return to execute the command.

```
Router# clock set 13:32:00 23 February 1997
```

Using the Command History Features

With the current Cisco IOS release, the user interface provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. With the command history feature, you can complete the tasks in the following sections:

- Set the Command History Buffer Size
- Recall Commands
- Disable the Command History Feature

Setting the Command History Buffer Size

By default, the system records 10 command lines in its history buffer. To set the number of command lines that the system will record during the current terminal session, use the following command in EXEC mode:

Command	Purpose
terminal history [<i>size number-of-lines</i>]	Enable the command history feature for the current terminal session.

The **terminal no history size** command resets the number of lines saved in the history buffer to the default of 10 lines.

To configure the number of command lines the system will record for all sessions on a particular line, use the following command in line configuration mode:

Command	Purpose
history [<i>size number-of-lines</i>] ¹	Enable the command history feature.

1. The **no history** command turns off command history for the line.

Recalling Commands

To recall commands from the history buffer, use one of the following commands:

Command	Purpose
Press Ctrl-P or the up arrow key. ¹	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press Ctrl-N or the down arrow key. ¹	Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.
show history	While in EXEC mode, list the last several commands you have just entered.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Disabling the Command History Feature

The command history feature is automatically enabled. To disable it during the current terminal session, use the following EXEC mode command:

Command	Purpose
terminal no history	Disable the command history feature for the current session.

To configure a specific line so that the command history feature is disabled, use the following command in line configuration mode:

Command	Purpose
no history	Configure the line so that the command history feature is disabled.

Using the No and Default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function. Use the command without the keyword **no** to reenable a disabled feature or to enable a feature that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** form of the **ip routing** command. To reenable it, use the plain **ip routing** form. The Cisco IOS software command reference publications provide the complete syntax for every configuration command and describes what the **no** form of a command does (when a **no** form is available).

Using Command-Line Editing Features and Shortcuts

There are a variety of shortcuts and editing features enabled for the Cisco IOS command-line interface. The following subsections describe these features:

- Enable Enhanced Editing Mode
- Move Around on the Command Line
- Complete a Partial Command Name
- Paste in Buffer Entries

- Edit Command Lines that Wrap
- Delete Entries
- Scroll Down a Line or a Screen
- Redisplay the Current Command Line
- Transpose Mistyped Characters
- Control Capitalization
- Designate a Keystroke as a Command Entry
- Disable Enhanced Editing Mode

Using Capital Letters when Entering Commands

Note You can enter commands in uppercase, lowercase, or mixed case. Only passwords are case sensitive. However, throughout it is a Cisco IOS documentation convention to always present commands in lowercase.

Moving Around on the Command Line

Use the following commands to move the cursor around on the command line to make corrections or changes:

Step	Keystrokes	Purpose
1	Press Ctrl-B or press the left arrow key. ¹	Move the cursor back one character.
2	Press Ctrl-F or press the right arrow key. ¹	Move the cursor forward one character.
3	Press Ctrl-A .	Move the cursor to the beginning of the command line.
4	Press Ctrl-E .	Move the cursor to the end of the command line.
5	Press Esc B .	Move the cursor back one word.
6	Press Esc F .	Move the cursor forward one word.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Completing a Partial Command Name

If you cannot remember a complete command name, press the Tab key to allow the system to complete a partial entry. To do so, use the following command:

Keystrokes	Purpose
Enter the first few letters and press the Tab key.	Complete a command name.

If your keyboard does not have a Tab key, press **Ctrl-I** instead.

In the following example, when you enter the letters **conf** and press the Tab key, the system provides the complete command:

```
Router# conf<Tab>
```

```
Router# configure
```

If you enter a set of characters that could indicate more than one command, the system beeps to indicate an error. Enter a question mark (?) to obtain a list of commands that begin with that set of characters. Do not leave a space between the last letter you enter and the question mark (?).

For example, there are three commands in privileged mode that start with `co`. To see what they are, type `co?` at the privileged EXEC prompt:

```
Router# co?
configure connect copy
Router# co
```

Pasting in Buffer Entries

The system provides a buffer that contains the last 10 items you deleted. To recall these items and paste them in the command line, use the following commands:

Step	Keystrokes	Purpose
1	Press Ctrl-Y .	Recall the most recent entry in the buffer.
2	Press Esc Y .	Recall the next buffer entry.

The buffer contains only the last 10 items you have deleted or cut. If you press **Esc Y** more than 10 times, you will cycle back to the first buffer entry.

Editing Command Lines that Wrap

The enhanced editing provides a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts 10 spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. To scroll back, use the following command:

Keystrokes	Purpose
Press Ctrl-B or the left arrow key repeatedly until you scroll back to the beginning of the command entry, or press Ctrl-A to return directly to the beginning of the line. ¹	Return to the beginning of a command line to verify that you have entered a lengthy command correctly.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

In the following example, the `access-list` command entry extends beyond one line. When the cursor first reaches the end of the line, the line is shifted 10 spaces to the left and redisplayed. The dollar sign (\$) indicates that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted 10 spaces to the left.

```
Router(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
Router(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
Router(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
Router(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

When you have completed the entry, press **Ctrl-A** to check the complete syntax before pressing the Return key to execute the command. The dollar sign (\$) appears at the end of the line to indicate that the line has been scrolled to the right:

```
Router(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

The Cisco IOS software assumes you have a terminal screen that is 80 columns wide. If you have a width other than that, use the **terminal width** command to set the width of your terminal.

Use line wrapping in conjunction with the command history feature to recall and modify previous complex command entries. See the section “Recall Commands” in this chapter for information about recalling previous command entries.

Deleting Entries

Use any of the following commands to delete command entries if you make a mistake or change your mind:

Keystrokes	Purpose
Press the Delete or Backspace key.	Erase the character to the left of the cursor.
Press Ctrl-D .	Delete the character at the cursor.
Press Ctrl-K .	Delete all characters from the cursor to the end of the command line.
Press Ctrl-U or Ctrl-X .	Delete all characters from the cursor to the beginning of the command line.
Press Ctrl-W .	Delete the word to the left of the cursor.
Press Esc D .	Delete from the cursor to the end of the word.

Scrolling Down a Line or a Screen

When you use the help facility to list the commands available in a particular mode, the list is often longer than the terminal screen can display. In such cases, a More prompt is displayed at the bottom of the screen, assuming that the **length** or **terminal length** command is configured correctly. To view the next line or screen, use the following commands:

Keystrokes	Purpose
Press the Return key.	Scroll down one line.
Press the Space bar.	Scroll down one screen.

Note The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the keystrokes listed above whenever you see the More prompt.

Redisplaying the Current Command Line

If you are entering a command and the system suddenly sends a message to your screen, you can easily recall your current command line entry. To do so, use the following command:

Keystrokes	Purpose
Press Ctrl-L or Ctrl-R .	Redisplay the current command line.

Transposing Mistyped Characters

If you have mistyped a command entry, you can transpose the mistyped characters by using the following command:

Keystrokes	Purpose
Press Ctrl-T .	Transpose the character to the left of the cursor with the character located at the cursor.

Controlling Capitalization

You can capitalize or lowercase words or capitalize a set of letters with simple keystroke sequences. To do so, use the following commands:

Keystrokes	Purpose
Press Esc C .	Capitalize at the cursor.
Press Esc L .	Change the word at the cursor to lowercase.
Press Esc U .	Capitalize letters from the cursor to the end of the word.

Designating a Keystroke as a Command Entry

Sometimes you might want to use a particular keystroke as an executable command, perhaps as a shortcut. Use the following keystroke to insert a system code for this purpose:

Keystrokes
Press Ctrl-V or Esc Q .

Disabling and Reenabling Enhanced Editing Features

The above editing features were introduced in Cisco IOS Release 9.21, and are automatically enabled on your system. However, there may be some unique situations which could warrant disabling these enhanced editing features. For example, you may have prebuilt scripts that conflict with enhanced editing functionality. To globally disable enhanced editing mode and revert to the editing mode of software releases before Cisco IOS release 9.21, use the following command in line configuration mode:

Command	Purpose
no editing	Disable the enhanced editing features for a particular line.

To disable enhanced editing mode for the current terminal session, use the following command in EXEC mode:

Command	Purpose
terminal no editing	Disable the enhanced editing features for the local line.

You can reenable enhanced editing mode with the **editing** command or **terminal editing** command.

To reenable the enhanced editing mode for the current terminal session, use the following command in EXEC mode:

Command	Purpose
terminal editing	Enable the enhanced editing features for the current terminal session.

To reconfigure a specific line to have enhanced editing mode, use the following command in line configuration mode:

Command	Purpose
<code>editing</code>	Enable the enhanced editing features.

Summary of Cisco IOS Configuration Modes

This section contains summaries of the other configuration modes not mentioned in the “Summary of the Main Cisco IOS Command Modes” on page 22. For specific information on any particular configuration mode, see the documentation references given in the following summaries:

- Access-List Configuration Mode
- APPN Configuration Modes
- CAS-Custom Configuration Mode
- Certificate Authorities Configuration Mode
- Certificate Chain Configuration Mode
- Controller Configuration Mode
- Crypto Map Configuration Mode
- Crypto Transform Configuration Mode
- Dial-Peer Configuration Mode
- Hex Input Mode
- Hub Configuration Mode
- IBM Channel Attach Configuration Modes
 - Interface Channel Configuration Mode
 - Internal LAN Configuration Mode
 - Internal Adapter Configuration Mode
- Interface-ATM-VC Configuration Mode
- IPX-Router Configuration Mode
- ISAKMP Policy Configuration Mode
- Key Chain Configuration Mode
 - Key Chain Key Configuration Mode
- LANE Database Configuration Mode
- Line Configuration Mode
- Map-Class Configuration Mode
- Map-List Configuration Mode
- Modem Pool Configuration Mode
- MPC Configuration Mode

- MPS Configuration Mode
- Poll-Group Configuration Mode
- Public Key Configuration Mode
 - Public Key Chain Configuration Mode
- Response Time Reporter Configuration Mode
- Route-Map Configuration Mode
- Router Configuration Mode
- TN3270 Server Command Modes
- VC-Class Configuration Mode
- Voice-Port Configuration Mode

Most of these modes can be entered from global configuration mode. In these modes, the **exit** command returns you to the global configuration mode. Other modes must be entered from another configuration mode. Entering the **exit** command in one of these modes returns you to the configuration mode you used to enter the mode.

In any configuration mode, to enter privileged EXEC mode and leave configuration mode entirely, use the **end** command or press **Ctrl-Z**.

Table 2 in the “Summary of Configuration Command Modes” section lists how to enter each mode.

Access-List Configuration Mode

All IP and IPX access lists can be identified by a number. Alternatively, some IP and IPX access lists can be identified by a name. Use access-list configuration mode when you are creating a named IP or IPX access list.

For information on creating a named IP access list, refer to the “Configuring IP Services” chapter in the *Network Protocols Configuration Guide, Part 1*. For information on creating a named IPX access list, refer to the “Configuring Novell IPX” chapter in the *Network Protocols Configuration Guide, Part 2*.

APPN Configuration Modes

Advanced Peer-to-Peer Networking (APPN) is the second generation of SNA. APPN provides support for client/server applications and offers more dynamics than traditional hierarchical SNA, such as dynamic directory and routing services.

APPN allows you to define attributes of the APPN network that can become quite complex. To easily manage the details of APPN, special configuration command modes and conventions have been developed.

Because APPN offers a large number of configuration options, specific configuration dialogs are used for each major APPN configuration item. When you define the major item, you will automatically enter the detailed configuration mode for that item. There are two options to exit the detailed configuration mode. Use the **complete** command to exit the detailed configuration mode and update the APPN subsystem with the changes. Use the **exit** command to leave the definition in “no complete” state without updating the APPN subsystem.

Refer to the “APPN Configuration Commands” chapter in the *Bridging and IBM Networking Command Reference* for information on the following APPN modes:

- APPN Control Point Mode

- APPN Port Mode
- APPN Link Station Mode
- APPN Connection Network Mode
- APPN Class of Service Mode
- APPN Mode Configuration Mode
- APPN Partner LU Location Mode
- APPN Subsystem Mode

CAS-Custom Configuration Mode

R2 signaling is an international signaling standard common to channelized E1 networks. However, there is no single signaling standard for R2. The ITU-T Q.400-Q.490 recommendation defines R2, but a number of countries and geographic regions implement R2 in entirely different ways.

Use CAS-custom configuration mode to customize E1 R2 signaling parameters for a particular E1 channel group on a channelized E1 line. Some switches require you to fine tune your R2 settings. However, do not tamper with these special signaling commands unless you understand exactly how your switch will be effected.

For more information, refer to the “Channelized E1 and Channelized T1” chapter in the *Dial Solutions Configuration Guide*.

Certificate Authorities Configuration Mode

Performing the **crypto ca identity** command puts you into the ca-identity configuration mode. In this mode you can specify characteristics for certificate authorities (CAs).

Certificate Chain Configuration Mode

The **crypto ca certificate chain** global configuration command puts you into certificate chain configuration mode. In this mode you can delete certificates using the **certificate** command.

Controller Configuration Mode

You can configure channelized T1 in the controller configuration mode. Refer to the “Configuring Channelized E1 and Channelized T1” chapter in the *Dial Solutions Configuration Guide* for more information.

Crypto Map Configuration Mode

Use crypto map configuration mode to create or alter the definition of a crypto-map. Crypto-maps are part of an authentication/encryption router configuration. For more information, refer to the “Configuring Cisco Encryption Technology” chapter in the *Security Configuration Guide*.

Crypto Transform Configuration Mode

Using the **crypto ipsec transform-set** command puts you into crypto transform configuration mode. While in this mode you can change the initialization vector length for the esp-rfc1829 transform, or you can change the mode to tunnel or transport.

Dial-Peer Configuration Mode

Use dial-peer configuration mode to configure dial peers for Voice over IP, Voice over ATM, Voice over Frame Relay, and Voice over HDLC. For more information, refer to the chapters on these technologies in the *Voice, Video, and Home Applications Configuration Guide*.

Hex Input Mode

Use hex input mode to enter a public key for an encrypting peer router. The public key data is entered in hexadecimal form, and it will take more than one command line to enter. To continue entering the public key data on a new line, press Return. When the public key is completely entered, press Return to get a new line, then type **quit** to return to the global configuration mode. For more information, refer to the “Configuring Cisco Encryption Technology” chapter in the *Security Configuration Guide*.

Hub Configuration Mode

Hub configuration commands configure hub functionality for an Ethernet interface on the Cisco 2500. They always follow a **hub** global configuration command. Refer to the “Configuring LAN Interfaces” chapter in this publication.

IBM Channel Attach Configuration Modes

The Channel Interface Processor (CIP) supports the IBM channel attach feature. This configuration is an ideal connectivity hub for large corporate networks that provide routing services between mainframes and LANs.

Interface Channel Configuration Mode

Before you configure your channel attach interface, you must select an interface. The following mode is valid only for port 2 on a CIP board. Ports 0 and 1 represent real, physical ports. Port 2 is an internal, virtual port. Refer to the “IBM Channel Attach Commands” chapter in the *Bridging and IBM Networking Command Reference*.

Internal LAN Configuration Mode

Use the IBM channel internal LAN configuration mode to configure an internal LAN on a CIP interface and configure Cisco Systems Network Architecture (CSNA) parameters. Refer to the “IBM Channel Attach Commands” chapter in the *Bridging and IBM Networking Command Reference*.

Internal Adapter Configuration Mode

Internal adapter commands allow you to configure the link characteristics for the internal LAN adapter and name the internal LAN adapter. Refer to the “IBM Channel Attach Commands” chapter in the *Bridging and IBM Networking Command Reference*.

To configure an internal adapter interface, you must first use the bridge-group internal LAN configuration command or the source-bridge internal LAN configuration command to configure bridging type. These commands are documented in the “Source-Route Bridging Commands” chapter of the *Bridging and IBM Networking Command Reference*.

Interface-ATM-VC Configuration Mode

When you create an ATM PVC or SVC, you will enter the interface-ATM-VC configuration sub-mode which allows you to configure various parameters that will apply when the VC is active. For configuration information, refer to the ATM configuration chapters of the *Wide-Area Networking Configuration Guide*.

IPX-Router Configuration Mode

Internet Packet Exchange (IPX) is a Novell network-layer protocol. The IPX-router configuration mode is used to configure IPX routing. Refer to the “Novell IPX Commands” chapter in the *Network Protocols Command Reference, Part 2*

ISAKMP Policy Configuration Mode

When you enter the **crypto isakmp policy** command, you are put into the ISAKMP policy configuration command mode. In this mode, you can specify IKE policy parameters.

Key Chain Configuration Mode

From key chain configuration mode, you can manage authentication keys. For details on how to use key chain configuration commands, consult the “Configuring IP Routing Protocol-Independent Features” chapter of the *Network Protocols Configuration Guide, Part 1*.

Key management controls the authentication keys that routing protocols use. To enter key chain configuration mode, identify or define a key chain using the **keychain** command. From key chain configuration mode, you can identify or define key numbers.

Key Chain Key Configuration Mode

Once you define a key chain, use the key chain key configuration mode to configure the keys on the key chain. Refer to the “IP Routing Protocol-Independent Commands” chapter in the *Network Protocols Command Reference, Part 1*.

LANE Database Configuration Mode

LAN emulation (LANE) clients consult the LANE configuration server for information such as the location of the LANE server. The configuration server looks up the configuration information in its name database.

A LANE database contains entries that bind an emulated LAN name to the ATM address of the LANE server, bind LANE client MAC addresses to an emulated LAN name, and bind LANE client ATM address templates to an emulated LAN name.

In LANE database configuration mode, you can use the **client-atm-address name**, **default name**, **mac-address name**, and **name server-atm-address** commands to create entries in the specified database.

Refer to the “LAN Emulation Commands” chapter of the *Cisco IOS Switching Services Command Reference*.

Line Configuration Mode

Line configuration commands modify the operation of an auxiliary, console, physical, or virtual terminal line. Line configuration commands always follow a **line** command, which defines a line number. These commands are generally used to connect to remote routers or access servers, change terminal parameter settings either on a line-by-line basis or for a range of line, and set up the auxiliary port modem configuration to support dial-on-demand routing (DDR). See the “Configuring Modem Support and Asynchronous Devices” chapter in the *Dial Solutions Configuration Guide*.

Map-Class Configuration Mode

Cisco IOS Frame Relay software allows you to specify parameters that control the traffic that the source router will send over a switched virtual circuit (SVC). Use the map-class configuration mode to configure these parameters. For configuration information, see the “Configure a Map Class” section in the “Configuring Frame Relay” chapter of the *Wide-Area Networking Configuration Guide*.

Map-List Configuration Mode

Cisco IOS Frame Relay software supports static mapping schemes that identify the protocol addresses of remote hosts or routers. Use the map-list configuration mode to define the protocol addresses and associate each protocol address with a specific map class. For configuration information, see the “Configuring Frame Relay” chapter in the *Wide-Area Networking Configuration Guide*.

Modem Pool Configuration Mode

A modem pool is a group of modems inside an access server that are assigned a single dialed number identification service number (DNIS). After you enter modem pool configuration mode, you can create multiple pools of physical modems, assign unique DNIS numbers to each modem pool, and set maximum simultaneous connect limits.

For more information, refer to the “Managing Modems” chapter in the *Dial Solutions Configuration Guide*.

MPC Configuration Mode

When you configure/create an MPOA client (MPC), you automatically enter the MPC configuration mode. Using the MPC configuration mode is optional. You can use the MPC configuration mode only when you need to change certain operating parameters. If you choose not to change any parameters, just exit and the default values will be used.

Refer to the “MPOA Commands” chapter of the *Cisco IOS Switching Services Command Reference*.

MPS Configuration Mode

When you configure/create an MPOA server (MPS), you automatically enter the MPS configuration mode. Using the MPS configuration mode is optional. You can use the MPS configuration mode only when you need to change certain operating parameters. If you choose not to change any parameters, just exit and the default values will be used.

Refer to the “MPOA Commands” chapter of the *Cisco IOS Switching Services Command Reference*.

Poll-Group Configuration Mode

Use the **syscon poll-group** command to enable data collection for a specific poll group. The poll-group configuration mode is required for Performance Data Collection, which allows a system controller to collect and store SNMP MIB data from its managed router and dial shelves.

You can enter any of the following commands while in poll-group configuration mode:

- **enable (poll-group configuration)**
- **oid**
- **poll-interval**
- **samples**
- **shelf-type**
- **transfer-mode**

You must specify the desired Object IDs and the transfer mode. If you do not specify the **shelf-type** command, the system controller collects data from all discovered shelves. The default data collection interval is 10 minutes. The default maximum number of samples is 10. To begin the data collection process, specify the **enable** command.

See the “System Controller Commands” chapter in the *Configuration Fundamentals Command Reference* for more information about poll group configuration mode.

Public Key Configuration Mode

Using the **addressed-key** or **named-key** public key chain configuration commands puts you into public key configuration mode. In this mode you can specify RSA or DSS public keys.

Public Key Chain Configuration Mode

Using the **crypto key pubkey-chain rsa** command puts you into public key chain configuration mode. In this mode, you can manually specify other IPsec peers’ RSA or DSS public keys.

Response Time Reporter Configuration Mode

Use the response time reporter configuration mode to configure a probe to measure response times and availability. Refer to the “Monitoring the Router and Network” chapter in the *Configuration Fundamentals Configuration Guide*.

Route-Map Configuration Mode

Use the route-map configuration mode to configure routing table and source and destination information. See the “Configuring IP Routing Protocol-Independent Features” chapter in the *Network Protocols Configuration Guide, Part 1*.

Router Configuration Mode

Router configuration commands configure an IP routing protocol and always follow a **router** command. See the relevant chapter on your IP routing protocol in the *Network Protocols Configuration Guide, Part 1*.

TN3270 Server Configuration Modes

The TN3270 server provides a set of configuration modes. The TN3270 server can be configured only on Port 2, the internal LAN port, of a Channel Interface Processor (CIP) card.

Note These commands are documented in the “Configuring IBM Channel Attach” chapter in the *Bridging and IBM Networking Configuration Guide* and the “IBM Channel Attach Commands” chapter in the *Bridging and IBM Networking Command Reference*.

The following are the TN3270 server command modes:

- TN3270 server configuration mode
- DLUR configuration mode
- DLUR SAP configuration mode
- PU configuration mode

VC-Class Configuration Mode

A VC class is a set of preconfigured VC parameters that you configure and apply to a particular VC or ATM interface. You may apply a VC class to an ATM main interface, subinterface, PVC or SVC. For example, you can create a VC class that contains VC parameter configurations that you will apply to a particular PVC or SVC. You might create another VC class that contains VC parameter configurations that you will apply to all VCs configured on a particular ATM main interface or subinterface.

Use VC-class configuration mode to configure a set of VC parameters that will apply to an ATM main interface, subinterface, PVC, or SVC. For information on configuring a VC class, refer to the “Configure VC Classes” section in one of the following ATM chapters in the *Wide-Area Networking Configuration Guide*:

- Configuring ATM on the AIP for Cisco 7500 Series Routers
- Configuring ATM on the ATM Port Adapter for Cisco 7200 & 7500 Series Routers
- Configuring ATM on the ATM-CES Port Adapter for Cisco 7200 Series Routers
- Configuring ATM on the Enhanced ATM Port Adapter for Cisco 7200 & 7500 Series Routers
- Configuring ATM on the NPM for Cisco 4500 and 4700 Routers
- Configuring ATM on the 1-Port ATM-25 Network Module

Voice-Port Configuration Mode

Use voice port configuration mode to configure voice port settings on the Cisco 3600 and Cisco MC3810. For more information, refer to the Configuring Voice Ports chapter in the *Cisco IOS Solutions for Voice, Video, and Home Applications Configuration Guide*.

Summary of Configuration Command Modes

Table 2 lists the command modes covered in this section, how to access and exit each mode, the prompt while in each mode, and an example of how to get to the mode.

Note The exit method is only listed if the **exit** command does not return you to global configuration mode or you must use a different command to exit the mode.

The prompts listed assume that the default device name of “Router” is in use.

Table 43 Configuration Command Modes

Command Mode	Access and Exit Method	Prompt	Example
Access-list configuration	From global configuration mode, use the ip access-list or ipx access-list command. ip access-list {standard extended} name or ipx access-list {standard extended sap summary} name	Router (config-std-nacl) # or Router (config-ext-nacl) #	Router (config) # ip access-list extended flag Router (config-ext-nacl) #
APPN configuration	From global configuration mode, use the appn mode command.	Router (appn) #	Router (config) # appn mode Router (appn) #
Ca-identity configuration	From global configuration mode, use the crypto ca identity command.	Router (ca-identity) #	Router (config) # crypto ca identity Router (ca-identity) #
CAS custom configuration	From controller E1 configuration mode, use the cas-custom channel command.	Router (config-ctrl-cas) #	Router (config-controller) # cas-custom 1 router (config-ctrl-cas) # ? CAS custom commands: ani-digits answer-signal caller-digits ...
Certificate chain configuration	From global configuration mode, use the crypto ca certificate chain command.	Router (config-cert-chain) #	Router (config) # crypto ca certificate Router (config-cert-chain) #
Controller configuration	From global configuration mode, use the controller t1 slot/port command to configure a channelized T1 interface.	Router (config-controller) #	Router (config) # controller t1 0/0 Router (config-controller) #
Crypto map configuration	From global configuration mode, use the crypto map map-name [seq-num] command.	Router (config-crypto-map) #	Router (config) # crypto map Research 10 Router (config-crypto-map) #
Crypto transform configuration	From global configuration mode, use the crypto ipsec transform-set command.	Router (config-crypto-trans) #	Router (config) # crypto ipsec transform-set Router (config-crypto-trans) #
Dial peer voice configuration	From global configuration mode, use the dial peer voice tag {pots voip vofr voatm vohdlc} command.	Router (config-dialpeer) #	Router (config) # dial peer voice 1 pots Router (config-dialpeer) #

Table 43 Configuration Command Modes (Continued)

Command Mode	Access and Exit Method	Prompt	Example
Hex input	From global configuration mode, use the crypto public-key command. crypto public-key <i>key-name serial-number</i> To exit hex input mode, use the quit command.	Router (config-pubkey) #	Router (config) # crypto public-key BananaCryptoEngine 01709644 Enter a public key as a hexadecimal number ... Router (config-pubkey) # C31260F4 BD8A5ACE 2C1B1E6C 8B0ABD27 01493A50 Router (config-pubkey) # A6A66946 Router (config-pubkey) # quit Router (config) #
Hub configuration	From global configuration mode, enter by specifying a hub with the hub <i>number port [port]</i> command.	Router (config-hub) #	Router (config) # hub ethernet 0 1 3 Router (config-hub) #
Interface-ATM -VC configuration	From interface configuration mode, use the pvc <i>vpi/vci</i> or svc nsap <i>address</i> command.	Router (config-if-atm-vc) #	Router (config-if) # pvc 0/33 Router (config-if-atm-vc) # or Router (config-if) # svc nsap AB.CDEF.01.234567.890A.BCDE.F012.34 56.7890.1234.12 Router (config-if-atm-vc) #
Interface channel configuration	From global configuration mode, use the interface channel <i>slot/port</i> command.	Router (config) #	Router (config) # interface channel 0/1 Router (config) #
Internal LAN configuration	From interface configuration mode, use the lan [ethernet tokenring fdi] <i>lan-id</i> command. To exit to interface configuration mode, use the exit command.	Router (config-if) #	Router (config) # lan ethernet 10 Router (cfg-lan-Ether 10) #
Internal adapter configuration	From internal LAN configuration mode, enter the adapter <i>adapter-number mac-address</i> command. To exit to Internal LAN configuration mode, use the exit command.	Router (config-lan) #	Router (config) # lan ethernet 10 Router (cfg-lan-Ether 10) # adapter 1 4.5.6 Router (cfg-adap-Ether 10-1) #
IPX-router configuration	From global configuration mode, enter by issuing the ipx routing command, then a command that begins with ipx router (such as ipx router eigrp). ipx router (eigrp <i>autonomous-system-number</i> nlsp [<i>tag</i>] rip)	Router (config-ipx-router) #	Router (config) # ipx router rip Router (config-ipx-router) #
ISAKMP policy configuration	From global configuration mode, use the crypto isakmp policy command.	Router (config-isakmp) #	Router (config) # crypto isakmp policy Router (config-isakmp) #

Table 43 Configuration Command Modes (Continued)

Command Mode	Access and Exit Method	Prompt	Example
Key chain configuration	From global configuration mode, use the keychain command. keychain <i>name-of-chain</i>	Router (config-keychain) #	Router (config) # keychain blue Router (config-keychain) #
Key chain key configuration	From key chain configuration mode, use the key number command. To exit to key chain configuration mode, use the exit command.	Router (config-keychain-key) #	Router (config) # keychain blue Router (config-keychain) # key 10 Router (config-keychain-key) #
LANE database configuration	From global configuration mode, use the lane database command. lane database [<i>database-name</i>]	Router (lane-config-datab) #	Router (config) # lane database red Router (lane-config-datab) #
Line configuration	From global configuration mode, enter by specifying a line with a line { <i>aux</i> <i>con</i> <i>tty</i> <i>vty</i> } <i>line-number</i> [<i>ending-line-number</i>] command.	Router (config-line) #	Router (config) # line vty 0 4 Router (config-line) #
Map-class configuration	From global configuration mode, configure a map class with the map-class encapsulation class-name command.	Router (config-map-class) #	Router (config) # map-class atm aaa Router (config-map-class) #
Map-list configuration	From global configuration mode, define a map list with the map-list name command.	Router (config-map-list) #	Router (config) # map-list atm Router (config-map-list) #
Modem pool configuration	From global configuration mode, use the modem-pool name command.	Router (config-modem-pool) #	Router (config) # modem-pool v90service Router (config-modem-pool) # pool-range 30-50 Router (config-modem-pool) # called-number 2000 Router (config-modem-pool) # exit Router (config)
MPC configuration mode	From global configuration mode, use the mpoa client config name command.	Router (config) #	Router (config) # mpoa client config name ip_mpc Router (mpoa-client-config) #
MPS configuration mode	From global configuration mode, use the mpoa server config name command.	Router (config) #	Router (config) # mpoa server config name ip_mps Router (mpoa-server-config) #
Poll-group configuration	From global configuration mode, enter poll-group configuration mode with the syscon poll-group command.	Router (config-poll-gr) #	Router (config) # syscon poll-group cmlineinfo Router (config-poll-gr) #

Table 43 Configuration Command Modes (Continued)

Command Mode	Access and Exit Method	Prompt	Example
Public key configuration	Using the addressed-key or named-key public key chain configuration commands puts you into public key configuration mode. In this mode you can specify RSA or DSS public keys.	Router (config-pubkey) #	Router (config) # addressed-key Router (config-pubkey) #
Public key chain configuration	From global configuration mode, enter public key chain configuration mode with the crypto key pubkey-chain rsa command .	Router (config-pubkey-key) #	Router (config) # crypto key pubkey-chain rsa Router (config-pubkey-key) #
Response time reporter configuration	From global configuration mode, use the rtr command. rtr probe	Router (config-rtr) #	Router (config) # rtr 1 Router (config-rtr) #
Route-map configuration	From global configuration mode, enter by specifying the route-map [map-tag] command.	Router (config-route-map) #	Router (config) # route-map arizona Router (config-route-map) #
Router configuration	From global configuration mode, enter by issuing the router [keyword] command (such as router igrp).	Router (config-router) #	Router (config) # router rip Router (config-router) #
TN3270 server configuration	From interface configuration mode, use the tn3270-server command. To exit to interface configuration mode, use the exit command.	Router (tn3270-server) #	Router (config) # tn3270-server Router (tn3270-server) #
DLUR configuration	From TN3270 configuration mode, use the dlur command. To exit to TN3270 configuration mode, use the exit command.	Router (tn3270-dlur) #	Router (config) # tn3270-server Router (tn3270-server) # dlur Router (tn3270-dlur) #
DLUR SAP configuration	From DLUR configuration mode, use the lsap command. To exit to DLUR configuration mode, use the exit command.	Router (tn3270-dlur-sap) #	Router (config) # tn3270-server Router (tn3270-server) # dlur Router (tn3270-dlur) # lsap Router (tn3270-dlur-sap) #
PU configuration	From TN3270 server configuration mode or from DLUR configuration mode, use the PU command. To exit PU configuration mode, use the exit command.	Router (tn3270-pu) # Router (tn3270-dlur-pu) #	Router (config) # tn3270-server Router (tn3270-server) # pu PU1 05d00001 10.0.0.1 token-adapter 1 8 rmac 4000.0000.0001 rsap 4 Router (tn3270-pu) #
VC-class configuration	From interface configuration mode, use the vc-class atm name command.	Router (config-vc-class) #	Router (config-if) # vc-class atm pvcl Router (config-vc-class) #
Voice-port configuration	From global configuration mode, enter by issuing the voice port slot/sub-unit/port command for the Cisco 3600 series, or voice port slot/port for the Cisco MC3810.	Router (config-voiceport) #	Router (config) # voice port 1/1/2 Router (config-voiceport)

