

stopbits

To set the number of the stop bits transmitted per byte, use the **stopbits** command in line configuration mode. To restore the default value, use the **no** form of this command.

```
stopbits {1 | 1.5 | 2}
```

```
no stopbits
```

Syntax Description		
	1	One stop bit.
	1.5	One and one-half stop bits.
	2	Two stop bits. This is the default.

Defaults 2 stop bits per byte

Command Modes Line configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Communication protocols provided by devices such as terminals and modems often require a specific stop-bit setting.

Examples In the following example, the stop bits transmitted per byte are changed from the default of two stop bits to one stop bit as a performance enhancement for line 4:

```
Router(config)# line 4
Router(config-line)# stopbits 1
```

Related Commands	Command	Description
	terminal stopbits	Changes the number of stop bits sent per byte by the current terminal line during an active session.

system (ERM policy)

To configure system level resource owners, use the **system** command in ERM policy configuration mode.

system

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes ERM policy configuration

Command History	Release	Modification
	12.3(14)T	This command was introduced.

Usage Guidelines You can configure system level resources in ERM policy configuration mode.

Examples The following example shows how to configure system level ROs:

```
Router(config-erm-policy)# system
```

Related Commands	Command	Description
	buffer public	Enters the buffer owner configuration mode and sets thresholds for buffer usage.
	cpu interrupt	Enters the CPU owner configuration mode and sets thresholds for interrupt level CPU utilization.
	cpu process	Enters the CPU owner configuration mode and sets thresholds for processor level CPU utilization.
	cpu total	Enters the CPU owner configuration mode and sets thresholds for total CPU utilization.
	critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
	major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
	memory io	Enters the memory owner configuration mode and sets threshold values for I/O memory.
	memory processor	Enters the memory owner configuration mode and sets threshold values for processor memory.
	minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
	policy (ERM)	Configures an ERM resource policy.

Command	Description
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.

tag

To create a user-specified identifier for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **tag** command in the appropriate submode of IP SLA monitor configuration or RTR configuration mode. To remove a tag from an operation, use the **no tag** form of this command.

tag *text*

no tag

Syntax Description

<i>text</i>	Name of a group to which the operation belongs from 0 to 16 ASCII characters.
-------------	---

Defaults

No tag identifier is specified.

Command Modes

IP SLA Monitor Configuration

DHCP configuration (config-sla-monitor-dhcp)
 DLSw configuration (config-sla-monitor-dlsw)
 DNS configuration (config-sla-monitor-dns)
 Frame Relay configuration (config-sla-monitor-frameRelay)
 FTP configuration (config-sla-monitor-ftp)
 HTTP configuration (config-sla-monitor-http)
 ICMP echo configuration (config-sla-monitor-echo)
 ICMP path echo configuration (config-sla-monitor-pathEcho)
 ICMP path jitter configuration (config-sla-monitor-pathJitter)
 TCP connect configuration (config-sla-monitor-tcp)
 UDP echo configuration (config-sla-monitor-udp)
 UDP jitter configuration (config-sla-monitor-jitter)
 VoIP configuration (config-sla-monitor-voip)

RTR Configuration

DHCP configuration (config-rtr-dhcp)
 DLSw configuration (config-rtr-dlsw)
 DNS configuration (config-rtr-dns)
 Frame Relay configuration (config-rtr-frameRelay)
 FTP configuration (config-rtr-ftp)
 HTTP configuration (config-rtr-http)
 ICMP echo configuration (config-rtr-echo)
 ICMP path echo configuration (config-rtr-pathEcho)
 ICMP path jitter configuration (config-rtr-pathJitter)
 TCP connect configuration (config-rtr-tcp)
 UDP echo configuration (config-rtr-udp)
 UDP jitter configuration (config-rtr-jitter)



Note

The configuration mode varies depending on the Cisco IOS release you are running and the operation type configured. See the “Usage Guidelines” section for more information.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

An operation tag is normally used to logically link operations in a group.

Tags can be used to support automation (for example, by using the same tag for two different operations on two different routers echoing the same target).

IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 181](#)). You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation.

The configuration mode for the **tag** command varies depending on the Cisco IOS release you are running (see [Table 181](#)) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the ICMP echo operation type is configured, you would enter the **tag** command in ICMP echo configuration mode (config-sla-monitor-echo) within IP SLA monitor configuration mode.

Table 181 Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.3(14)T and 12.4	ip sla monitor	IP SLA monitor configuration
All other Cisco IOS releases	rtr	RTR configuration

Examples

In the following examples, IP SLAs ICMP echo operation 1 is tagged with the label testoperation. Note that the Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 181](#)).

IP SLA Monitor Configuration

```
ip sla monitor 1
  type echo protocol ipIcmpEcho 172.16.1.176
  tag testoperation
!
ip sla monitor schedule 1 life forever start-time now
```

RTR Configuration

```
rtr 1
  type echo protocol ipIcmpEcho 172.16.1.176
  tag testoperation
!
rtr schedule 1 life forever start-time now
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
rtr	Begins configuration for an IP SLAs operation and enters RTR configuration mode.

tclsh

To enable the interactive Tool Command Language (Tcl) shell, use the **tclsh** command in privileged EXEC mode.

tclsh

Syntax Description This command has no arguments or keywords.

Defaults The Tcl shell is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.3(2)T	This command was introduced.

Usage Guidelines Use the **tclsh** command when you want to run Tcl commands from the Cisco IOS command-line interface (CLI). When the interactive Tcl shell is enabled and Tcl configuration mode is entered, Tcl commands can be entered line by line or a predefined Tcl script can be run. After Tcl commands are entered they are sent to a Tcl interpreter. If the commands are recognized as valid Tcl commands, the command is executed and the result is sent to the tty. If a command is not a recognized Tcl command, it is sent to the Cisco IOS CLI parser. If the command is not a Tcl or Cisco IOS command, two error messages will be displayed.

A predefined Tcl script can be created outside of Cisco IOS software, transferred to Flash or disk memory, and run within Cisco IOS software. It is also possible to create a Tcl script and precompile the code before running it under Cisco IOS.

Use the Cisco IOS CLI **exit** or the Tcl **tclquit** command to disable the use of the Tcl shell and return to privileged EXEC mode.

Examples The following example shows how to enable the Tcl interactive shell:

```
Router# tclsh
Router(tcl)#
```

Related Commands	Command	Description
	scripting tcl encdir	Specifies the default location of external encoding files used by the Tcl shell.
	scripting tcl init	Specifies an initialization script for the Tcl shell.

template (cns)

To specify a list of Cisco Networking Services (CNS) connect templates within a CNS connect profile to be applied to a router's configuration, use the **template** command in CNS connect configuration mode. To disable this CNS connect template, use the **no** form of this command.

template *name* [...*name*]

no template *name* [...*name*]

Syntax Description

<i>name</i>	Name of the CNS connect template to be applied to a router's configuration. The ellipsis (...) in the command syntax indicates that the command input can include multiple <i>name</i> arguments. Multiple <i>name</i> arguments are delimited by a single space.
-------------	---

Defaults

No CNS connect templates are specified.

Command Modes

CNS connect configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9).

Usage Guidelines

First use the **cns connect** command to enter CNS connect configuration mode and define the parameters of a CNS connect profile for connecting to the CNS configuration engine. Then use the following CNS connect commands to create a CNS connect profile:

- **discover**
- **template**

A CNS connect profile specifies the **discover** commands and associated **template** commands that are to be applied to a router's configuration. The **template** command specifies the list of CNS connect templates that is to be applied to a router's configuration. The templates in the list are applied one at a time. That is, when the **template** command is processed, the first template in the list is applied to the router's configuration. The router then tries to ping the CNS configuration engine. If the ping fails, then the first template in the list is removed from the router's configuration and the second template in the list is applied and so on.

The configuration mode in which the CNS connect templates are applied is specified by the immediately preceding **discover** command. (If there are no preceding **discover** commands, the templates are applied in global configuration mode.) When multiple **discover** and **template** commands are configured in a CNS connect profile, they are processed in the order in which they are entered.

Examples

The following example shows how to create a CNS connect profile named profile-1:

```
Router (config)# cns connect profile-1
Router (config-cns-conn)# discover interface Serial
Router (config-cns-conn)# template temp-A1 temp-A2
Router (config-cns-conn)# template temp-B1 temp-B2
Router (config-cns-conn)# exit
Router (config)#
```

In this example, the following sequence of events occur for all serial interfaces when the **cns connect profile-1** command is processed. Assume all ping attempts to the CNS configuration engine are unsuccessful.

1. Enter interface configuration mode and apply all commands in the temp-A1 template to the router's configuration.
2. Enter interface configuration mode and apply all commands in the temp-B1 template to the router's configuration.
3. Try to ping the CNS configuration engine.
4. Enter interface configuration mode and remove all commands in the temp-B1 template from the router's configuration.
5. Enter interface configuration mode and apply all commands in the temp-B2 template to the router's configuration.
6. Try to ping the CNS configuration engine.
7. Enter interface configuration mode and remove all commands in the temp-B2 template from the router's configuration.
8. Enter interface configuration mode and remove all commands in the temp-A1 template from the router's configuration.
9. Enter interface configuration mode and apply all commands in the temp-A2 template to the router's configuration.
10. Enter interface configuration mode and apply all commands in the temp-B1 template to the router's configuration.
11. Try to ping the CNS configuration engine.
12. Enter interface configuration mode and remove all commands in the temp-B1 template from the router's configuration.
13. Enter interface configuration mode and apply all commands in the temp-B2 template to the router's configuration.
14. Try to ping the CNS configuration engine.
15. Enter interface configuration mode and remove all commands in the temp-B2 template from the router's configuration.
16. Enter interface configuration mode and remove all commands in the temp-A2 template from the router's configuration.

Related Commands

Command	Description
cli (cns)	Specifies the command lines of a CNS connect template.
cns connect	Enters CNS connect configuration mode and defines the parameters of a CNS connect profile for connecting to the CNS configuration engine.

Command	Description
cns template connect	Enters CNS template connect configuration mode and defines the name of a CNS connect template.
discover (cns)	Defines the interface parameters within a CNS connect profile for connecting to the CNS configuration engine.

terminal databits

To change the number of data bits per character for the current terminal line for this session, use the **terminal databits** command in EXEC mode.

terminal databits {5 | 6 | 7 | 8}

Syntax Description	5	Six data bits per character.
	6	Six data bits per character.
	7	Seven data bits per character.
	8	Eight data bits per character. This is the default.

Defaults 8 data bits per character

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Communication protocols provided by devices such as terminals and modems often require a specific data bit setting. The **terminal databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity generation is in effect, specify 8 data bits per character. The other keywords (**5** and **6**) are supplied for compatibility with older devices and are generally not used.

Examples In the following example, the databits per character is changed to seven for the current session:

```
Router# terminal databits 7
```

Related Commands	Command	Description
	databits	Sets the number of data bits per character that are interpreted and generated by the router hardware.
	terminal parity	Defines the generation of the parity bit for the current terminal line and session.

terminal data-character-bits

To set the number of data bits per character that are interpreted and generated by the Cisco IOS software for the current line and session, use the **terminal data-character-bits** command in EXEC mode.

terminal data-character-bits {7 | 8}

Syntax Description	7	Seven data bits per character.
	8	Eight data bits. This is the default.

Defaults 8 data bits per character

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command is used primarily to strip parity from X.25 connections on routers with the protocol translation software option. The **terminal data-character-bits** command does not work on hard-wired lines.

Examples The following example sets the data bits per character to seven on the current line:

```
Router# terminal data-character-bits 7
```

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 dispatch-character

To define a character that causes a packet to be sent for the current session, use the **terminal dispatch-character** command in EXEC mode.

```
terminal dispatch-character ascii-number [ascii-number2 . . . ascii-number]
```

Syntax Description		
<i>ascii-number</i>		The ASCII decimal representation of the character, such as Return (ASCII character 13) for line-at-a-time transmissions.
<i>ascii-number2</i> . . . <i>ascii-number</i>		(Optional) Additional decimal representations of characters. This syntax indicates that you can define any number of characters as dispatch characters.

Command Modes	
	EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	
	At times, you might want to queue up a string of characters until they fill a complete packet and then transmit the packet to a remote host. This can make more efficient use of a line, because the access server or router normally dispatches each character as it is entered.

Examples	
	The following example defines the characters Ctrl-D (ASCII decimal character 4) and Ctrl-Y (ASCII decimal character 25) as the dispatch characters: Router# terminal dispatch-character 4 25

Related Commands	Command	Description
	dispatch-character	Defines a character that causes a packet to be sent.

terminal dispatch-timeout

To set the character dispatch timer for the current terminal line for the current session, use the **terminal dispatch-timeout** command in EXEC mode.

terminal dispatch-timeout *milliseconds*

Syntax Description	<i>milliseconds</i>	Integer that specifies the number of milliseconds that the router waits after it puts the first character into a packet buffer before sending the packet. During this interval, more characters can be added to the packet, which increases the processing efficiency of the remote host.
---------------------------	---------------------	---

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines

Use this command to increase the processing efficiency of the remote host.

The **dispatch-timeout** line configuration command causes the software to buffer characters into packets for transmission to the remote host. The Cisco IOS software sends a packet a specified amount of time after the first character is put into the buffer. You can use the **terminal dispatch-timeout** and **terminal dispatch-character** line configuration commands together. In this case, the software dispatches a packet each time the dispatch character is entered, or after the specified dispatch timeout interval, depending on which condition is met first.



Note

The router response time might appear intermittent if the timeout interval is greater than 100 milliseconds and remote echoing is used.

Examples

In the following example, the dispatch timeout timer is set to 80 milliseconds:

```
Router# terminal dispatch-timeout 80
```

Related Commands

Command	Description
dispatch-timeout	Sets the character dispatch timer for a specified line or group of lines.

terminal download

To temporarily set the ability of a line to act as a transparent pipe for file transfers for the current session, use the **terminal download** command in EXEC mode.

terminal download

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines You can use this feature to run a program such as KERMIT, XMODEM, or CrossTalk that downloads a file across an access server or router line. This command configures the terminal line to send data and is equivalent to entering all the following commands:

- [terminal telnet transparent](#)
- **terminal no escape-character** (see [terminal escape-character](#))
- **terminal no hold-character** (see [terminal hold-character](#))
- **terminal no padding 0** (see [terminal padding](#))
- **terminal no padding 128** (see [terminal padding](#))
- [terminal parity none](#)
- [terminal databits 8](#)

Examples The following example configures a line to act as a transparent pipe:

```
Router# terminal download
```

terminal editing

To reenble the enhanced editing mode for only the current terminal session, use the **terminal editing** command in EXEC mode. To disable the enhanced editing mode on the current line, use the **no** form of this command.

terminal editing

terminal no editing

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command is identical to the **editing** EXEC mode command, except that it controls (enables or disables) enhanced editing for only the terminal session you are using. For a description of the available editing keys, see the description of the **editing** command in this document.

Examples In the following example, enhanced editing mode is reenbled for only the current terminal session:

```
Router> terminal editing
```

Related Commands	Command	Description
	editing	Controls CLI enhanced editing features for a particular line.

terminal escape-character

To set the escape character for the current terminal line for the current session, use the **terminal escape-character** command in EXEC mode.

terminal escape-character *ascii-number*

Syntax Description	<i>ascii-number</i>	ASCII decimal representation of the escape character or control sequence (for example, Ctrl-P).
---------------------------	---------------------	---

Defaults	Ctrl-^ (Ctrl-Shift-6)
-----------------	-----------------------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines See the [“ASCII Character Set and Hexidecimal Values”](#) appendix for a list of ASCII characters and their numerical representation.

This command is useful, for example, if you have the default escape character defined for a different purpose in your keyboard file. Entering the escape character followed by the X key returns you to EXEC mode when you are connected to another computer.



Note

The Break key generally cannot be used as an escape character on the console terminal because the operating software interprets the Break command on a console line as an instruction to halt the system.

Examples In the following example, the escape character to Ctrl-P (ASCII decimal character 16) for the current session:

```
Router# terminal escape-character 16
```

Related Commands	Command	Description
	escape-character	Defines a system escape character.

terminal exec-character-bits

To locally change the ASCII character set used in EXEC and configuration command characters for the current session, use the **terminal exec-character-bits** command in EXEC mode.

terminal exec-character-bits {7 | 8}

Syntax Description	7	Selects the 7-bit ASCII character set. This is the default.
	8	Selects the full 8-bit character set.

Defaults 7-bit ASCII character set (unless set otherwise in global configuration mode)

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This EXEC command overrides the **default-value exec-character-bits** global configuration command. Configuring the EXEC character width to 8 bits enables you to view special graphical and international characters in banners, prompts, and so on.

When the user exits the session, the character width is reset to the default value established by the **exec-character-bits** global configuration command. However, setting the EXEC character width to 8 bits can also cause failures. For example, if a user on a terminal that is sending parity enters the **help** command, an “unrecognized command” message appears because the system is reading all 8 bits, and the eighth bit is not needed for the **help** command.

Examples The following example temporarily configures the system to use a full 8-bit user interface for system banners and prompts, allowing the use of additional graphical and international characters:

```
Router# terminal exec-character-bits 8
```

Related Commands	Command	Description
	exec-character-bits	Configures the character widths of EXEC and configuration command characters.

terminal flowcontrol

To set flow control for the current terminal line for the current session, use the **terminal flowcontrol** command in EXEC mode.

terminal flowcontrol { **none** | **software** [**in** | **out**] | **hardware** }

Syntax Description	
none	Prevents flow control.
software	Sets software flow control.
in out	(Optional) Specifies the direction of flow control: in causes the router to listen to flow control from the attached device, and out causes the router to send flow control information to the attached device. If you do not specify a direction, both directions are assumed.
hardware	Sets hardware flow control. For information about setting up the EIA/TIA-232 line, see the manual that was shipped with your product.

Command Modes	
	EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	
	Flow control enables you to regulate the rate at which data can be transmitted from one point so that it is equal to the rate at which it can be received at another point. Flow control protects against loss of data because the terminal is not capable of receiving data at the rate it is being sent. You can set up data flow control for the current terminal line in one of two ways: software flow control, which you do with control key sequences, and hardware flow control, which you do at the device level.
	For software flow control, the default stop and start characters are Ctrl-S and Ctrl-Q (XOFF and XON). You can change them with the terminal stop-character and terminal start-character EXEC commands.

Examples	
	In the following example, incoming software flow control is set for the current session:
	Router# terminal flowcontrol software in

Related Commands	Command	Description
	flowcontrol	Sets the method of data flow control between the terminal or other serial device and the router.

terminal full-help

To get help for the full set of user-level commands, use the **terminal full-help** command in EXEC mode.

terminal full-help

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The **terminal full-help** command enables a user to see all of the help messages available from the terminal. It is used with the **show ?** command.

Examples In the following example, the difference between the output of the **show ?** command before and after using the **terminal full-help** command is shown:

```
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
compress      Show compression statistics.
.
.
.
x25           X.25 information
xns           XNS information
xremote       XRemote statistics

```

Related Commands

Command	Description
full-help	Gets help for the full set of user-level commands.
help	Displays a brief description of the help system.

terminal history

To enable the command history function with 10 lines for the current terminal session, use the **terminal history** command in user EXEC or privileged EXEC mode. To disable the command history function, use the **no** form of this command.

terminal history

terminal no history

Syntax Description This command has no arguments or keywords.

Defaults Enabled, history buffer of 10 lines

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The history function provides a record of commands you have entered. This function is particularly useful for recalling long or complex commands or entries for the purposes of modifying them slightly and reexecuting them.

The **terminal history** command enables the command history function with the default buffer size or the last buffer size specified using the **terminal history size** command.

[Table 182](#) lists the keys and functions you can use to recall commands from the history buffer.

Table 182 History Keys

Key(s)	Function
Ctrl-P or Up Arrow ¹	Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or Down Arrow ¹	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands.

1. The arrow keys function only with ANSI-compatible terminals.

Examples In the following example, the command history feature is disabled for the current terminal session:

```
Router> terminal no history
```

Related Commands	Command	Description
	history	Enables the command history function, or changes the command history buffer size for a particular line.
	show history	Lists the commands you have entered in the current EXEC session.
	terminal history size	Sets the size of the history buffer for the command history feature for the current terminal session.

terminal history size

To change the size of the command history buffer for the current terminal session, use the **terminal history size** command in EXEC mode. To reset the command history buffer to its default size of 10 lines, use the **no** form of this command.

terminal history size *number-of-lines*

terminal no history size

Syntax Description	<i>number-of-lines</i>	Number of command lines that the system will record in its history buffer. The range is from 0 to 256. The default is 10.
---------------------------	------------------------	---

Defaults	10 lines of command history
-----------------	-----------------------------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The history feature provides a record of commands you have entered. This feature is particularly useful for recalling long or complex commands or entries for the purposes of modifying them slightly and reissuing them.

The **terminal history size** command enables the command history feature and sets the command history buffer size. The **terminal no history size** command resets the buffer size to the default of 10 command lines.

[Table 183](#) lists the keys and functions you can use to recall commands from the history buffer. When you use these keys, the commands recalled will be from EXEC mode if you are in EXEC mode, or from all configuration modes if you are in any configuration mode.

Table 183 History Keys

Key	Function
Ctrl-P or Up Arrow ¹	Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or Down Arrow ¹	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands.

1. The arrow keys function only with ANSI-compatible terminals.

In EXEC mode, you can also use the **show history** command to show the contents of the command history buffer.

To check the current settings for the command history feature on your line, use the **show line** command.

Examples

In the following example, the number of command lines recorded is set to 15 for the current terminal session. The user then checks to see what line he/she is connected to using the **show users** command. The user uses this line information to issue the show line command. (In this example, the user uses the **show begin** option in the **show line** command to start the output at the “Editing is enabled/disabled” line.)

```
Router# terminal history size 15
Router# show users

      Line      User      Host(s)      Idle      Location
* 50 vty 0      admin      idle         00:00:00
! the * symbol indicates the active terminal session for the user (line 50)

Router# show line 50 | begin Editing

Editing is enabled.
! the following line shows the history settings for the line
History is enabled, history size is 15.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed transports are telnet. Preferred is none.
No output characters are padded
No special data dispatching characters
```

Related Commands

Command	Description
history	Enables the command history function, or changes the command history buffer size for a particular line.
show <command> begin	Searches the output of any show command and displays the output from the first instance of a specified string.
show history	Lists the commands you have entered in the current EXEC session.
terminal history	Enables the command history feature for the current terminal session.

terminal hold-character

To define the hold character for the current session, use the **terminal hold-character** command in EXEC mode. To return the hold character definition to the default, use the **no** form of this command.

terminal hold-character *ascii-number*

terminal no hold-character

Syntax Description	<i>ascii-number</i>	ASCII decimal representation of a character or control sequence (for example, Ctrl-P).
--------------------	---------------------	--

Defaults The default hold character is defined by the **hold-character** global configuration command.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines You can define a local hold character that temporarily suspends the flow of output on the terminal. When information is scrolling too quickly, you can enter the hold character to pause the screen output, then enter any other character to resume the flow of output.

You cannot suspend output on the console terminal. To send the hold character to the host, precede it with the escape character.

Examples In the following example, the hold character for the current (local) session is set to Ctrl-P. The **show terminal** output is included to show the verification of the setting (the value for the hold character is shown in the “Special Characters” listing).

```
Router# terminal hold-character 16
"^P" is the local hold character
Router# show terminal
Line 50, Location: "", Type: "VT220"
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600
Status: PSI Enabled, Ready, Active, No Exit Banner, Automore On
Capabilities: none
Modem state: Ready
Group codes: 0
Special Chars: Escape Hold Stop Start Disconnect Activation
                ^^x    ^P    -    -    none
Timeouts:      Idle EXEC Idle Session Modem Answer Session Dispatch
                00:10:00 never          none          not set
                Idle Session Disconnect Warning
                never
                Login-sequence User Response
```

```
00:00:30
Autoselect Initial Wait
not set

Modem type is unknown.
Session limit is not set.
Time since activation: 00:04:13
Editing is enabled.
History is enabled, history size is 10.
.
.
.
```

Related Commands

Command	Description
hold-character	Defines the local hold character used to pause output to the terminal screen.
show terminal	Displays settings for terminal operating characteristics.

terminal international

If you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji) and print the Escape character as a single character instead of as the caret and bracket symbols (^[]) for a current Telnet session, use the **terminal international** command in user EXEC or privileged mode. To display characters in 7-bit format for a current Telnet session, use the **no** form of this command.

terminal international

no terminal international

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines If you are configuring a Cisco IOS platform using the Cisco web browser UI, this feature is enabled automatically when you enable the Cisco web browser UI using the **ip http server** global configuration command.

Examples The following example enables a Cisco IOS platform to display 8-bit and multibyte characters and print the Escape character as a single character instead of as the caret and bracket symbols (^[]) when you are using Telnet to access the platform for the current Telnet session:

```
Router# terminal international
```

Related Commands	Command	Description
	international	Prints the Escape character as a single character instead of as the caret and bracket symbols (^[]) in instances when you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji).

terminal keymap-type

To specify the current keyboard type for the current session, use the **terminal keymap-type** command in EXEC mode.

terminal keymap-type *keymap-name*

Syntax Description	<i>keymap-name</i> Name defining the current keyboard type.
---------------------------	---

Defaults	VT100
-----------------	-------

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

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	You must use this command when you are using a keyboard other than the default of VT100.
-------------------------	--

Examples	The following example specifies a VT220 keyboard as the current keyboard type:
-----------------	--

```
Router# terminal keymap-type vt220
```

Related Commands	Command	Description
	show keymap	Displays the current keymap settings.

terminal length

To set the number of lines on the current terminal screen for the current session, use the **terminal length** command in EXEC mode.

terminal length *screen-length*

Syntax Description	<i>screen-length</i>	Number of lines on the screen. A value of zero disables pausing between screens of output.
---------------------------	----------------------	--

Defaults	24 lines
-----------------	----------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The system uses the length value to determine when to pause during multiple-screen output. A value of zero prevents the router from pausing between screens of output.

Some types of terminal sessions do not require you to specify the screen length because the screen length specified can be learned by some remote hosts. For example, the rlogin protocol uses the screen length to set up terminal parameters on a remote UNIX host.

Examples In the following example, the system is configured to prevent output from pausing if it exceeds the length of the screen:

```
Router# terminal length 0
```

Related Commands	Command	Description
	length	Sets the terminal screen length.

terminal monitor

To display **debug** command output and system error messages for the current terminal and session, use the **terminal monitor** command in EXEC mode.

terminal monitor

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes EXEC

Release	Modification
10.0	This command was introduced.

Usage Guidelines Remember that all terminal parameter-setting commands are set locally and do not remain in effect after a session is ended.

Examples In the following example, the system is configured to display **debug** command output and error messages during the current terminal session:

```
Router# terminal monitor
```

terminal notify

To enable terminal notification about pending output from other Telnet connections for the current session, use the **terminal notify** command in EXEC mode. To disable notifications for the current session, use the **no** form of this command.

terminal notify

terminal no notify

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Enabling notifications may be useful if, for example, you want to know when another connection receives mail, or when a process has been completed.

This command enables or disables notifications for only the current session. To globally set these notifications, use the **notify** line configuration command.

Examples In the following example, notifications will be displayed to inform the user when output is pending on another connection:

```
Router# terminal notify
```

Related Commands	Command	Description
	notify	Enables terminal notification about pending output from other Telnet connections.

terminal padding

To change the character padding on a specific output character for the current session, use the **terminal padding** command in EXEC mode.

terminal padding *ascii-number count*

Syntax Description	<i>ascii-number</i>	ASCII decimal representation of the character.
	<i>count</i>	Number of NULL bytes sent after the specified character, up to 255 padding characters in length.

Defaults No padding

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Character padding adds a number of null bytes to the end of the string and can be used to make a string an expected length for conformity.

Use this command when the attached device is an old terminal that requires padding after certain characters (such as ones that scrolled or moved the carriage). See the [“ASCII Character Set and Hexidecimal Values”](#) appendix for a list of ASCII characters.

Examples The following example pads Ctrl-D (ASCII decimal character 4) with 164 NULL bytes:

```
Router# terminal padding 4 164
```

Related Commands	Command	Description
	padding	Sets the padding on a specific output character.

terminal parity

To define the generation of the parity bit for the current terminal line and session, use the **terminal parity** command in EXEC mode.

terminal parity { none | even | odd | space | mark }

Syntax Description	none	No parity. This is the default.
	even	Even parity.
	odd	Odd parity.
	space	Space parity.
	mark	Mark parity.

Defaults No parity.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Communication protocols provided by devices such as terminals and modems will sometimes require a specific parity bit setting. Refer to the documentation for your device to determine required parity settings.

Examples In the following example, odd parity checking is enabled for the current session:

```
Router# terminal parity odd
```

Related Commands	Command	Description
	parity	Defines generation of a parity bit for connections on a specified line or lines.

terminal rxspeed

To set the terminal receive speed (how fast information is sent to the terminal) for the current line and session, use the **terminal rxspeed** command in EXEC mode.

terminal rxspeed *bps*

Syntax Description	<i>bps</i> Baud rate in bits per second (bps). The default is 9600.
---------------------------	---

Defaults	9600 bps
-----------------	----------

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

Command History	Release	Modification
	10.0	

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

Examples	The following example sets the current auxiliary line receive speed to 115200 bps: Router# terminal rxspeed 115200
-----------------	--

Related Commands	Command	Description
		rxspeed
	terminal rxspeed	Sets the terminal receive speed for the current session.
	terminal txspeed	Sets the terminal transmit speed for a specified line or lines.
	terminal speed	Sets the transmit and receive speeds for the current session.

terminal special-character-bits

To change the ASCII character widths to accept special characters for the current terminal line and session, use the **terminal special-character-bits** command in EXEC mode.

terminal special-character-bits {7 | 8}

Syntax Description	7	Selects the 7-bit ASCII character set. This is the default.
	8	Selects the full 8-bit ASCII character set.

Defaults 7-bit ASCII character set

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines

Configuring the width to 8 bits enables you to use twice as many special characters as with the 7-bit setting. This selection enables you to add special graphical and international characters in banners, prompts, and so on.

This command is useful, for example, if you want the router to provide temporary support for international character sets. It overrides the **default-value special-character-bits** global configuration command and is used to compare character sets typed by the user with the special character available during a data connection, which includes software flow control and escape characters.

When you exit the session, character width is reset to the width established by the **default-value exec-character-bits** global configuration command.

Note that setting the EXEC character width to eight bits can cause failures. For example, if a user on a terminal that is sending parity enters the **help** command, an “unrecognized command” message appears because the Cisco IOS software is reading all eight bits, and the eighth bit is not needed for the **help** command.

Examples

The following example temporarily configures a router to use a full 8-bit user interface for system banners and prompts.

```
Router# terminal special-character-bits 8
```

Related Commands	Command	Description
	default-value exec-character-bits	Globally defines the character width as 7-bit or 8-bit.
	special-character-bits	Configures the number of data bits per character for special characters such as software flow control characters and escape characters.

terminal speed

To set the transmit and receive speeds of the current terminal line for the current session, use the **terminal speed** command in EXEC mode.

terminal speed *bps*

Syntax Description	<i>bps</i> Baud rate in bits per second (bps). The default is 9600.
---------------------------	---

Defaults	9600 bps
-----------------	----------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Set the speed to match the transmission rate of whatever device you have connected to the port. Some baud rates available on devices connected to the port might not be supported on the router. The router indicates whether the speed you selected is not supported.

Examples The following example restores the transmit and receive speed on the current line to 9600 bps:

```
Router# terminal speed 9600
```

Related Commands	Command	Description
	speed	Sets the terminal baud rate.

terminal start-character

To change the flow control start character for the current session, use the **terminal start-character** command in EXEC mode.

terminal start-character *ascii-number*

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

Defaults	Ctrl-Q (ASCII decimal character 17)
-----------------	-------------------------------------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	The flow control start character signals the start of data transmission when software flow control is in effect.
-------------------------	--

Examples	The following example changes the start character to Ctrl-O (ASCII decimal character 15): Router# terminal start-character 15
-----------------	---

Related Commands	Command	Description
	start-character	Sets the flow control start character.

terminal stopbits

To change the number of stop bits sent per byte by the current terminal line during an active session, use the **terminal stopbits** command in EXEC mode.

terminal stopbits {1 | 1.5 | 2}

Syntax Description

1	One stop bit.
1.5	One and one-half stop bits.
2	Two stop bits. This is the default.

Defaults

2 stop bits

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Communication protocols provided by devices such as terminals and modems often require a specific stop-bit setting.

Examples

In the following example, the setting for stop bits is changed to one for the current session:

```
Router# terminal stopbits 1
```

Related Commands

Command	Description
stopbits	Sets the number of the stop bits sent per byte.

terminal stop-character

To change the flow control stop character for the current session, use the **terminal stop-character** command in EXEC mode.

terminal stop-character *ascii-number*

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

Defaults	Ctrl-S (ASCII character decimal 19)
-----------------	-------------------------------------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	<p>The flow control stop character signals the end of data transmission when software flow control is in effect.</p> <p>See the “ASCII Character Set and Hexidecimal Values” appendix for a list of ASCII characters.</p>
-------------------------	---

Examples	<p>In the following example, the stop character is configured as Ctrl-E (ASCII character decimal 5) for the current session:</p>
-----------------	--

```
Router# terminal stop-character 5
```

Related Commands	Command	Description
	stop-character	Sets the flow control stop character.

terminal telnet break-on-ip

To cause an access server to generate a hardware Break signal when an interrupt-process (ip) command is received, use the **terminal telnet break-on-ip** command in EXEC mode.

terminal telnet break-on-ip

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The hardware Break signal occurs when a Telnet interrupt-process (ip) command is received on that connection. The **terminal telnet break-on-ip** command can be used to control the translation of Telnet interrupt-process commands into X.25 Break indications.



Note In this command, the acronym “ip” indicates “interrupt-process,” not Internet Protocol (IP).

This command is also a useful workaround in the following situations:

- Several user Telnet programs send an ip command, but cannot send a Telnet Break signal.
- Some Telnet programs implement a Break signal that sends an ip 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.

You can verify if this command is enabled with the **show terminal EXEC** command. If enabled the following line will appear in the output: `Capabilities: Send BREAK on IP.`

Examples In the following example, a Break signal is generated for the current connection when an interrupt-process command is issued:

```
Router# terminal telnet break-on-ip
```

Related Commands	Command	Description
	terminal telnet ip-on-break	Configures the system to send an interrupt-process (ip) signal when the Break command is issued.

terminal telnet refuse-negotiations

To configure the current session to refuse to negotiate full-duplex, remote echo options on incoming connections, use the **terminal telnet refuse-negotiations** command in EXEC mode.

terminal telnet refuse-negotiations

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines You can set the line to allow access server to refuse full-duplex, remote echo connection requests from the other end. This command suppresses negotiation of the Telnet Remote Echo and Suppress Go Ahead options.

Examples In the following example, the current session is configured to refuse full-duplex, remote echo requests:

```
Router# terminal telnet refuse-negotiations
```

terminal telnet speed

To allow an access server to negotiate transmission speed for the current terminal line and session, use the **terminal telnet speed** command in EXEC mode.

terminal telnet speed *default-speed maximum-speed*

Syntax Description		
<i>default-speed</i>	Line speed, in bits per second (bps), that the access server will use if the device on the other end of the connection has not specified a speed.	
<i>maximum-speed</i>	Maximum line speed in bits per second (bps), that the device on the other end of the connection can use.	

Defaults 9600 bps (unless otherwise set using the **speed**, **txspeed** or **rxspeed** line configuration commands)

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines You can match line speeds on remote systems in reverse Telnet, on host machines connected to an access server to access the network, or on a group of console lines connected to the access server when disparate line speeds are in use at the local and remote ends of the connections listed above. Line speed negotiation adheres to the Remote Flow Control option, defined in RFC 1080.



Note This command applies only to access servers. It is not supported on standalone routers.

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

```
Router# terminal telnet speed 2400 9600
```

terminal telnet sync-on-break

To cause the access server to send a Telnet Synchronize signal when it receives a Telnet Break signal on the current line and session, use the **terminal telnet sync-on-break** command in EXEC mode.

terminal telnet sync-on-break

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines You can configure the session to cause a reverse Telnet line to send a Telnet Synchronize signal when it receives a Telnet Break signal. The TCP Synchronize signal clears the data path, but still interprets incoming commands.



Note This command applies only to access servers. It is not supported on standalone routers.

Examples The following example sets an asynchronous line to cause the access server to send a Telnet Synchronize signal:

```
Router# terminal telnet sync-on-break
```

terminal telnet transparent

To cause 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, use the **terminal telnet transparent** command in EXEC mode.

terminal telnet transparent

Syntax Description This command has no arguments or keywords.

Defaults CR followed by an LF

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The end of each line typed at the terminal is ended with a Return (CR). This command permits interoperability with different interpretations of end-of-line demarcation in the Telnet protocol specification.



Note This command applies only to access servers. It is not supported on stand-alone routers.

Examples In the following example, the session is configured to send a CR signal as a CR followed by a NULL:
 Router# **terminal telnet transparent**

terminal terminal-type

To specify the type of terminal connected to the current line for the current session, use the **terminal terminal-type** command in EXEC mode.

terminal terminal-type *terminal-type*

Syntax Description	<i>terminal-type</i>	Defines the terminal name and type, and permits terminal negotiation by hosts that provide that type of service. The default is VT100.
---------------------------	----------------------	--

Defaults	VT100
-----------------	-------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	<p>Indicate the terminal type if it is different from the default of VT100.</p> <p>The terminal type name is used by TN3270s for display management and by Telnet and rlogin to inform the remote host of the terminal type.</p>
-------------------------	--

Examples	In the following example, the terminal type is defined as VT220 for the current session:
-----------------	--

```
Router# terminal terminal-type VT220
```

Related Commands	Command	Description
	terminal keymap-type	Specifies the current keyboard type for the current session.
	terminal-type	Specifies the type of terminal connected to a line.

terminal txspeed

To set the terminal transmit speed (how fast the terminal can send information) for the current line and session, use the **terminal txspeed** command in EXEC mode.

terminal txspeed *bps*

Syntax Description	<i>bps</i> Baud rate in bits per second (bps). The default is 9600 bps.
---------------------------	---

Defaults	9600 bps
-----------------	----------

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

Command History	Release	Modification
	10.0	This command was introduced.

Examples In the following example, the line transmit speed is set to 2400 bps for the current session:

```
Router# terminal txspeed 2400
```

Related Commands	Command	Description
	rxspeed	Sets the terminal receive speed for a specified line or lines.
	terminal rxspeed	Sets the terminal receive speed for the current line and session.
	terminal terminal-type	Specifies the type of terminal connected to the current line for the current session.
	txspeed	Sets the terminal transmit speed for a specified line or lines.

terminal width

To set the number of character columns on the terminal screen for the current line for a session, use the **terminal width** command in EXEC mode.

terminal width *characters*

Syntax Description

<i>characters</i>	Number of character columns displayed on the terminal. The default is 80 characters.
-------------------	--

Defaults

80 characters

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

By default, the route provides a screen display width of 80 characters. You can reset this value for the current session if it does not meet the needs of your terminal.

The rlogin protocol uses the value of the *characters* argument to set up terminal parameters on a remote host.

Examples

The following example sets the terminal character columns to 132:

```
Router# terminal width 132
```

Related Commands

Command	Description
width	Sets the terminal screen width (the number of character columns displayed on the attached terminal).

terminal-queue entry-retry-interval

To change the retry interval for a terminal port queue, use the **terminal-queue entry-retry-interval** command in global configuration mode. To restore the default terminal port queue interval, use the **no** form of this command.

terminal-queue entry-retry-interval *seconds*

no terminal-queue entry-retry-interval

Syntax Description	<i>seconds</i>	Number of seconds between terminal port retries. The default is 60 seconds.
---------------------------	----------------	---

Defaults	60 seconds
-----------------	------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines	If a remote device (such as a printer) is busy, the connection attempt is placed in a terminal port queue. If you want to decrease the waiting period between subsequent connection attempts, decrease the default of 60 to an interval of 10 seconds. Decrease the time between subsequent connection attempts when, for example, a printer queue stalls for long periods.
-------------------------	---

Examples	The following example changes the terminal port queue retry interval from the default of 60 seconds to 10 seconds:
-----------------	--

```
Router# terminal-queue entry-retry-interval 10
```

terminal-type

To specify the type of terminal connected to a line, use the **terminal-type** command in line configuration mode. To remove any information about the type of terminal and reset the line to the default terminal emulation, use the **no** form of this command.

terminal-type { *terminal-name* | *terminal-type* }

no terminal-type

Syntax Description		
	<i>terminal-name</i>	Terminal name.
	<i>terminal-type</i>	Terminal type.

Defaults VT100

Command Modes Line configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command records the type of terminal connected to the line. The *terminal-name* argument provides a record of the terminal type and allows terminal negotiation of display management by hosts that provide that type of service.

For TN3270 applications, this command must follow the corresponding ttycap entry in the configuration file.

Examples The following example defines the terminal on line 7 as a VT220:

```
Router(config)# line 7
Router(config-line)# terminal-type VT220
```

test flash

To test Flash memory on MCI and envm Flash EPROM interfaces, use the **test flash** command in EXEC mode.

test flash

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Examples In the following example, the Flash memory is tested:

```
test flash
```

Related Commands	Command	Description
	test interfaces	Tests the system interfaces on the modular router.
	test memory	Performs a test of Multibus memory (including nonvolatile memory) on the modular router.

test interfaces

To test the system interfaces on the modular router, use the **test interfaces** command in EXEC mode.

test interfaces

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The **test interfaces** EXEC command is intended for the factory checkout of network interfaces. It is not intended for diagnosing problems with an operational router. The **test interfaces** output does not report correct results if the router is attached to a “live” network. For each network interface that has an IP address that can be tested in loopback (MCI and ciscoBus Ethernet and all serial interfaces), the **test interfaces** command sends a series of ICMP echoes. Error counters are examined to determine the operational status of the interface.

Examples In the following example, the system interfaces are tested:

```
test interfaces
```

Related Commands	Command	Description
	test flash	Tests Flash memory on MCI and envm Flash EPROM interfaces.
	test memory	Performs a test of Multibus memory (including nonvolatile memory) on the modular router.

test memory

To perform a test of Multibus memory (including nonvolatile memory) on the modular router, use the **test memory** command in EXEC mode. The memory test overwrites memory.

test memory

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The memory test overwrites memory. If you use the **test memory** command, you will need to rewrite nonvolatile memory. For example, if you test Multibus memory, which is the memory used by the CSC-R 4-Mbps Token Ring interfaces, you will need to reload the system before the network interfaces will operate properly. The **test memory** command is intended primarily for use by Cisco personnel.

Examples In the following example, the memory is tested:

```
test memory
```

Related Commands	Command	Description
	test flash	Tests Flash memory on MCI and envm Flash EPROM interfaces.
	test interfaces	Tests the system interfaces on the modular router.

tftp-server

To configure a router or a Flash memory device on the router as a TFTP server, use one of the following **tftp-server** commands in global configuration mode. This command replaces the **tftp-server system** command. To remove a previously defined filename, use the **no** form of this command with the appropriate filename.

```
tftp-server flash [partition-number:]filename1 [alias filename2] [access-list-number]
```

```
tftp-server rom alias filename1 [access-list-number]
```

```
no tftp-server { flash [partition-number:]filename1 | rom alias filename2 }
```

Cisco 1600 Series and Cisco 3600 Series Routers

```
tftp-server flash [device:][partition-number:]filename
```

```
no tftp-server flash [device:][partition-number:]filename
```

Cisco 7000 Family Routers

```
tftp-server flash device:filename
```

```
no tftp-server flash device:filename
```

Syntax	Description
flash	Specifies TFTP service of a file in Flash memory.
rom	Specifies TFTP service of a file in ROM.
<i>filename1</i>	Name of a file in Flash or in ROM that the TFTP server uses in answering TFTP Read Requests.
alias	Specifies an alternate name for the file that the TFTP server uses in answering TFTP Read Requests.
<i>filename2</i>	Alternate name of the file that the TFTP server uses in answering TFTP Read Requests. A client of the TFTP server can use this alternate name in its Read Requests.
<i>access-list-number</i>	(Optional) Basic IP access list number. Valid values are from 0 to 99.
<i>partition-number:</i>	(Optional) Specifies TFTP service of a file in the specified partition of Flash memory. If the partition number is not specified, the file in the first partition is used. For the Cisco 1600 series and Cisco 3600 series routers, you must enter a colon after the partition number if a filename follows it.

<i>device:</i>	<p>(Optional) Specifies TFTP service of a file on a Flash memory device in the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers. The colon is required. Valid devices are as follows:</p> <ul style="list-style-type: none"> • flash—Internal Flash memory on the Cisco 1600 series and Cisco 3600 series routers. This is the only valid device for the Cisco 1600 series routers. • bootflash—Internal Flash memory in the Cisco 7000 family routers. • slot0—First PCMCIA slot on the Cisco 3600 series and Cisco 7000 family routers. • slot1—Second PCMCIA slot on the Cisco 3600 series and Cisco 7000 family. • slavebootflash—Internal Flash memory on the slave RSP card of a Cisco 7507 or Cisco 7513 router configured for HSA. • slaveslot0—First PCMCIA slot of the slave RSP card on a Cisco 7507 or Cisco 7513 router configured for HSA. • slaveslot1—Second PCMCIA slot of the slave RSP card on a Cisco 7507 or Cisco 7513 router configured for HSA.
<i>filename</i>	Name of the file on a Flash memory device that the TFTP server uses in answering a TFTP Read Request. Use this argument only with the Cisco 1600 series, Cisco 3600 series, Cisco 7000 series, or Cisco 7500 series routers.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

You can specify multiple filenames by repeating the **tftp-server** command. The system sends a copy of the system image contained in ROM or one of the system images contained in Flash memory to any client that issues a TFTP Read Request with this filename.

If the specified *filename1* or *filename2* argument exists in Flash memory, a copy of the Flash image is sent. On systems that contain a complete image in ROM, the system sends the ROM image if the specified *filename1* or *filename2* argument is not found in Flash memory.

Images that run from ROM cannot be loaded over the network. Therefore, it does not make sense to use TFTP to offer the ROMs on these images.

On the Cisco 7000 family routers, the system sends a copy of the file contained on one of the Flash memory devices to any client that issues a TFTP Read Request with its filename.

Examples

In the following example, the system uses TFTP to send a copy of the *version-10.3* file located in Flash memory in response to a TFTP Read Request for that file. The requesting host is checked against access list 22.

```
tftp-server flash version-10.3 22
```

In the following example, the system uses TFTP to send a copy of the ROM image *gs3-k.101* in response to a TFTP Read Request for the *gs3-k.101* file:

```
tftp-server rom alias gs3-k.101
```

In the following example, the system uses TFTP to send a copy of the *version-11.0* file in response to a TFTP Read Request for that file. The file is located on the Flash memory card inserted in slot 0.

```
tftp-server flash slot0:version-11.0
```

The following example enables a Cisco 3600 series router to operate as a TFTP server. The source file *c3640-i-mz* is in the second partition of internal Flash memory.

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# tftp-server flash flash:2:dirt/gate/c3640-i-mz
```

In the following example, the source file is in the second partition of the Flash memory PC card in slot 0 on a Cisco 3600 series:

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# tftp-server flash slot0:2:dirt/gate/c3640-j-mz
```

The following example enables a Cisco 1600 series router to operate as a TFTP server. The source file *c1600-i-mz* is in the second partition of Flash memory:

```
router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# tftp-server flash flash:2:dirt/gate/c1600-i-mz
```

Related Commands

Command	Description
access-list	Creates an extended access list.

tftp-server system

The **tftp-server system** command has been replaced by the **tftp-server** command. See the description of the [tftp-server](#) command in this chapter for more information.

threshold

To set the rising threshold (hysteresis) that generates a reaction event and stores history information for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **threshold** command in the appropriate submode of IP SLA monitor configuration or RTR configuration mode. To return to the default value, use the **no** form of this command.

threshold *milliseconds*

no threshold

Syntax Description	<i>milliseconds</i>	Number of milliseconds required for a rising threshold to be declared. The default value is 5000 ms.
---------------------------	---------------------	--

Defaults	5000 ms
-----------------	---------

Command Modes	IP SLA Monitor Configuration
	DHCP configuration (config-sla-monitor-dhcp) DLSw configuration (config-sla-monitor-dlsw) DNS configuration (config-sla-monitor-dns) Frame Relay configuration (config-sla-monitor-frameRelay) FTP configuration (config-sla-monitor-ftp) HTTP configuration (config-sla-monitor-http) ICMP echo configuration (config-sla-monitor-echo) ICMP path echo configuration (config-sla-monitor-pathEcho) ICMP path jitter configuration (config-sla-monitor-pathJitter) TCP connect configuration (config-sla-monitor-tcp) UDP echo configuration (config-sla-monitor-udp) UDP jitter configuration (config-sla-monitor-jitter) VoIP configuration (config-sla-monitor-voip)

RTR Configuration

DHCP configuration (config-rtr-dhcp)
 DLSw configuration (config-rtr-dlsw)
 DNS configuration (config-rtr-dns)
 Frame Relay configuration (config-rtr-frameRelay)
 FTP configuration (config-rtr-ftp)
 HTTP configuration (config-rtr-http)
 ICMP echo configuration (config-rtr-echo)
 ICMP path echo configuration (config-rtr-pathEcho)
 ICMP path jitter configuration (config-rtr-pathJitter)
 TCP connect configuration (config-rtr-tcp)
 UDP echo configuration (config-rtr-udp)
 UDP jitter configuration (config-rtr-jitter)



Note

The configuration mode varies depending on the Cisco IOS release you are running and the operation type configured. See the “Usage Guidelines” section for more information.

Command History

Release	Modification
11.2	This command was introduced.
12.3(7)T	The same functionality of this command was made available using the ip sla monitor reaction-configuration command.

Usage Guidelines

The value specified for the **threshold** command must not exceed the value specified for the **timeout** command.

IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 184](#)). You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation.

The configuration mode for the **threshold** command varies depending on the Cisco IOS release you are running (see [Table 184](#)) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the ICMP echo operation type is configured, you would enter the **threshold** command in ICMP echo configuration mode (config-sla-monitor-echo) within IP SLA monitor configuration mode.

Table 184 Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.3(14)T and 12.4	ip sla monitor	IP SLA monitor configuration
All other Cisco IOS releases	rtr	RTR configuration

Examples

In the following examples, the threshold of IP SLAs ICMP echo operation 1 is set to 2500 ms. Note that the Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 184](#)).

IP SLA Monitor Configuration

```
ip sla monitor 1
 type echo protocol ipIcmpEcho 172.16.1.176
 threshold 2500
!
ip sla monitor schedule 1 start-time now
```

RTR Configuration

```
rtr 1
 type echo protocol ipIcmpEcho 172.16.1.176
 threshold 2500
!
```

```
rtr schedule 1 start-time now
```

Related Commands	Command	Description
	ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
	rtr	Begins configuration for an IP SLAs operation and enters RTR configuration mode.
	timeout	Sets the amount of time the IP SLAs operation waits for a response from its request packet.

timeout

To set the amount of time a Cisco IOS IP Service Level Agreements (SLAs) operation waits for a response from its request packet, use the **timeout** command in the appropriate submode of IP SLA monitor configuration or RTR configuration mode. To return to the default value, use the **no** form of this command.

timeout *milliseconds*

no timeout

Syntax Description

<i>milliseconds</i>	Number of milliseconds (ms) the operation waits to receive a response from its request packet.
---------------------	--

Defaults

The default timeout value will vary depending on the type of IP SLAs operation you are configuring.

Command Modes

IP SLA Monitor Configuration

DHCP configuration (config-sla-monitor-dhcp)
 DLSw configuration (config-sla-monitor-dlsw)
 DNS configuration (config-sla-monitor-dns)
 Frame Relay configuration (config-sla-monitor-frameRelay)
 FTP configuration (config-sla-monitor-ftp)
 HTTP configuration (config-sla-monitor-http)
 ICMP echo configuration (config-sla-monitor-echo)
 ICMP path echo configuration (config-sla-monitor-pathEcho)
 ICMP path jitter configuration (config-sla-monitor-pathJitter)
 TCP connect configuration (config-sla-monitor-tcp)
 UDP echo configuration (config-sla-monitor-udp)
 UDP jitter configuration (config-sla-monitor-jitter)
 VoIP configuration (config-sla-monitor-voip)

RTR Configuration

DHCP configuration (config-rtr-dhcp)
 DLSw configuration (config-rtr-dlsw)
 DNS configuration (config-rtr-dns)
 Frame Relay configuration (config-rtr-frameRelay)
 FTP configuration (config-rtr-ftp)
 HTTP configuration (config-rtr-http)
 ICMP echo configuration (config-rtr-echo)
 ICMP path echo configuration (config-rtr-pathEcho)
 ICMP path jitter configuration (config-rtr-pathJitter)
 TCP connect configuration (config-rtr-tcp)
 UDP echo configuration (config-rtr-udp)
 UDP jitter configuration (config-rtr-jitter)

**Note**

The configuration mode varies depending on the Cisco IOS release you are running and the operation type configured. See the “Usage Guidelines” section for more information.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use the **timeout** command to set how long the operation waits to receive a response from its request packet, and use the **frequency** command to set the rate at which the IP SLAs operation restarts. The value specified for the **timeout** command cannot be greater than the value specified for the **frequency** command.

IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 185](#)). You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation.

The configuration mode for the **timeout** command varies depending on the Cisco IOS release you are running (see [Table 185](#)) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the ICMP echo operation type is configured, you would enter the **timeout** command in ICMP echo configuration mode (config-sla-monitor-echo) within IP SLA monitor configuration mode.

Table 185 Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.3(14)T and 12.4	ip sla monitor	IP SLA monitor configuration
All other Cisco IOS releases	rtr	RTR configuration

Examples

In the following examples, the timeout value for IP SLAs ICMP echo operation 1 is set for 2500 ms. Note that the Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 185](#)).

IP SLA Monitor Configuration

```
ip sla monitor 1
  type echo protocol ipIcmpEcho 172.16.1.176
  timeout 2500
!
ip sla monitor schedule 1 start-time now
```

RTR Configuration

```
rtr 1
  type echo protocol ipIcmpEcho 172.16.1.176
  timeout 2500
!
rtr schedule 1 start-time now
```

Related Commands	Command	Description
	frequency	Sets the rate at which the IP SLAs operation restarts.
	ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
	rtr	Begins configuration for an IP SLAs operation and enters RTR configuration mode.

time-period

To set the time increment for automatically saving an archive file of the current running configuration in the Cisco IOS configuration archive, use the **time-period** command in archive configuration mode. To disable this function, use the **no** form of this command.

time-period *minutes*

no time-period *minutes*

Syntax Description	<i>minutes</i>	Specifies how often, in minutes, to automatically save an archive file of the current running configuration in the Cisco IOS configuration archive.
---------------------------	----------------	---

Defaults	By default, no time increment is set.
-----------------	---------------------------------------

Command Modes	Archive configuration
----------------------	-----------------------

Command History	Release	Modification
	12.3(7)T	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines



Note

Before using this command, you must configure the **path** command in order to specify the location and filename prefix for the files in the Cisco IOS configuration archive.

If this command is configured, an archive file of the current running configuration is automatically saved after the given time specified by the *minutes* argument. Archive files will continue to be automatically saved at this given time increment until this function is disabled. Use the **maximum** command to set the maximum number of archive files of the running configuration to be saved.



Note

This command will save the current running configuration to the configuration archive whether or not the running configuration has been modified since the last archive file was saved.

Examples

In the following example, a value of 20 minutes is set as the time increment for which to automatically save an archive file of the current running configuration in the Cisco IOS configuration archive:

```
Router(config)# archive
Router(config-archive)# path disk0:myconfig
Router(config-archive)# time-period 20
```

Related Commands

Command	Description
archive config	Saves a copy of the current running configuration to the Cisco IOS configuration archive.
configure confirm	Confirms replacement of the current running configuration with a saved Cisco IOS configuration file.
configure replace	Replaces the current running configuration with a saved Cisco IOS configuration file.
maximum	Sets the maximum number of archive files of the running configuration to be saved in the Cisco IOS configuration archive.
path	Specifies the location and filename prefix for the files in the Cisco IOS configuration archive.
show archive	Displays information about the files saved in the Cisco IOS configuration archive.

time-range

To enable time-range configuration mode and define time ranges for functions (such as extended access lists), use the **time-range** command in global configuration mode. To remove the time limitation, use the **no** form of this command.

time-range *time-range-name*

no time-range *time-range-name*

Syntax Description	<i>time-range-name</i> Desired name for the time range. The name cannot contain a space or quotation mark, and must begin with a letter.
---------------------------	--

Defaults	None
-----------------	------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.0(1)T	This command was introduced.

Usage Guidelines The **time-range** entries are identified by a name, which is referred to by one or more other configuration commands. Multiple time ranges can occur in a single access list or other feature. After the **time-range** command, use the **periodic** time-range configuration command, the **absolute** time-range configuration command, or some combination of them to define when the feature is in effect. Multiple **periodic** commands are allowed in a time range; only one **absolute** command is allowed.



Tip

To avoid confusion, use different names for time ranges and named access lists.

Examples The following example denies HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m. The example allows UDP traffic on Saturday and Sunday from noon to midnight only.

```
time-range no-http
  periodic weekdays 8:00 to 18:00
!
time-range udp-yes
  periodic weekend 12:00 to 24:00
!
ip access-list extended strict
  deny tcp any any eq http time-range no-http
  permit udp any any time-range udp-yes
!
interface ethernet 0
  ip access-group strict in
```

Related Commands

Command	Description
absolute	Specifies an absolute start and end time for a time range.
ip access-list	Defines an IP access list by name.
periodic	Specifies a recurring (weekly) start and end time for a time range.
permit (IP)	Sets conditions under which a packet passes a named IP access list.

tos

To define a type of service (ToS) byte in the IP header of a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **tos** command in the appropriate submode of IP SLA monitor configuration or RTR configuration mode. To return to the default value, use the **no** form of this command.

tos *number*

no tos

Syntax Description

number Service type byte in the IP header. The range is 0 to 255. The default is 0.

Defaults

The default type-of-service value is 0.

Command Modes

IP SLA Monitor Configuration

HTTP configuration (config-sla-monitor-http)
 ICMP echo configuration (config-sla-monitor-echo)
 ICMP path echo configuration (config-sla-monitor-pathEcho)
 ICMP path jitter configuration (config-sla-monitor-pathJitter)
 TCP connect configuration (config-sla-monitor-tcp)
 UDP echo configuration (config-sla-monitor-udp)
 UDP jitter configuration (config-sla-monitor-jitter)

RTR Configuration

HTTP configuration (config-rtr-http)
 ICMP echo configuration (config-rtr-echo)
 ICMP path echo configuration (config-rtr-pathEcho)
 ICMP path jitter configuration (config-rtr-pathJitter)
 TCP connect configuration (config-rtr-tcp)
 UDP echo configuration (config-rtr-udp)
 UDP jitter configuration (config-rtr-jitter)



Note

The configuration mode varies depending on the Cisco IOS release you are running and the operation type configured. See the “Usage Guidelines” section for more information.

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

The ToS value is an 8-bit field in IP headers. This field contains information such as precedence and ToS. This information is useful for policy routing and for features like Committed Access Rate (CAR), where routers examine ToS values.

When the type of service is defined for an operation, the IP SLAs Responder will reflect the ToS value it receives.

IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 186](#)). You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation.

The configuration mode for the **tos** command varies depending on the Cisco IOS release you are running (see [Table 186](#)) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the ICMP echo operation type is configured, you would enter the **tos** command in ICMP echo configuration mode (config-sla-monitor-echo) within IP SLA monitor configuration mode.

Table 186 Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.3(14)T and 12.4	ip sla monitor	IP SLA monitor configuration
All other Cisco IOS releases	rtr	RTR configuration

Examples

In the following examples, IP SLAs operation 1 is configured as an ICMP echo operation with destination IP address 172.16.1.176. The ToS value is set to 0x80. Note that the Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 186](#)).

IP SLA Monitor Configuration

```
ip sla monitor 1
  type echo protocol ipIcmpEcho 172.16.1.176
  tos 0x80
!
ip sla monitor schedule 1 start-time now
```

RTR Configuration

```
rtr 1
  type echo protocol ipIcmpEcho 172.16.1.176
  tos 0x80
!
rtr schedule 1 start-time now
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
rtr	Begins configuration for an IP SLAs operation and enters RTR configuration mode.

traceroute

To discover the routes that packets will actually take when traveling to their destination address, use the **traceroute** command in user EXEC or privileged EXEC mode.

traceroute [**vrf** *vrf-name*] [*protocol*] *destination*

Syntax Description

vrf <i>vrf-name</i>	(Optional) Specifies the name of a Virtual Private Network (VPN) routing/forwarding instance table (VRF) in which to find the destination address. The only <i>protocol</i> argument keyword that you can select when you use the vrf <i>vrf-name</i> keyword-argument pair is the ip keyword.
<i>protocol</i>	(Optional) Protocol keyword, either appletalk , clns , ip , ipv6 , ipx , oldvines , or vines . When not specified, the <i>protocol</i> argument is based on an examination by the software of the format of the <i>destination</i> argument.
<i>destination</i>	(Optional in privileged EXEC mode; required in user EXEC mode) The destination address or host name for which you want to trace the route. The software determines the default parameters for the appropriate protocol and the tracing action begins.

Defaults

When not specified, the protocol argument is determined by the software examining the format of the *destination* argument. For example, if the software finds a *destination* argument in IP format, the protocol value defaults to IP.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The vrf <i>vrf-name</i> keyword and argument were added.
12.2(2)T, 12.0(21)ST, 12.0(22)S	Support for IPv6 was added.
12.2(11)T	The traceroute command test characters for IPv6 were updated. A new error message was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(5), 12.0(26)S1, 12.2(20)S	A line was added to the interactive traceroute vrf command, so that you can resolve the autonomous system (AS) number through the use of the global table or a VRF table, or you can choose not to resolve the AS.

Usage Guidelines

The **traceroute** command works by taking advantage of the error messages generated by routers when a datagram exceeds its hop limit value.

The **tracert** command starts by sending probe datagrams with a hop limit of 1. Including a hop limit of 1 with a probe datagram causes the neighboring routers to discard the probe datagram and send back an error message. The **tracert** command sends several probes with increasing hop limits and displays the round-trip time for each.

The **tracert** command sends out one probe at a time. Each outgoing packet might result in one or more error messages. A time-exceeded error message indicates that an intermediate router has seen and discarded the probe. A destination unreachable error message indicates that the destination node has received and discarded the probe because the hop limit of the packet reached a value of 0. If the timer goes off before a response comes in, the **tracert** command prints an asterisk (*).

The **tracert** command terminates when the destination responds, when the hop limit is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type **Ctrl-^ X**—by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

To use nondefault parameters and invoke an extended **tracert** test, enter the command without a *protocol* or *destination* argument in privileged EXEC mode. You are stepped through a dialog to select the desired parameters. Extended **tracert** tests are not supported in user EXEC mode. The user-level tracert feature provides a basic trace facility for users who do not have system privileges. The *destination* argument is required in user EXEC mode.

If the system cannot map an address for a host name, it returns a “%No valid source address for destination” message.

Resolving the AS with Interactive VRF Tracert

In the noninteractive mode, the **tracert vrf** command always resolves the AS in the global routing table. A destination address is required when you use the noninteractive command. Here, for example, the address is 10.0.0.3.

```
Router# tracert vrf green 10.0.0.3
```

In the interactive mode, a line in the **tracert vrf** command allows you to select the global routing table or VRF table to resolve the AS number of a host address or to choose not to resolve the AS:

```
Resolve AS number in (G)lobal table, (V)RF or(N)one [G]:
```

If you do not select one of these options to resolve the AS, the AS is resolved in the global routing table (default behavior).

The following example shows you the line where you select the routing table option that best represents the configuration of your network:

```
Router# tracert vrf green

Protocol [ip]:
Target IP address: 10.0.0.3
Source address:
Numeric display [n]:
Resolve AS number in (G)lobal table, (V)RF or(N)one [G]:VRF
Timeout in seconds [3]:
. . .
```



Note

IP is the only protocol that you can select for a destination address when you use the **tracert vrf** command.

If you select **N(one)**, the AS is not resolved, and the AS is not indicated in the output of the command. For example:

```
Tracing the route to 10.0.0.3
```

```

1 10.1.1.9 [MPLS: Labels 25/45 Exp 0] 4 msec 0 msec 0 msec
2 10.1.1.1 [MPLS: Labels 26/45 Exp 0] 0 msec 4 msec 0 msec
3 10.12.1.101 [MPLS: Labels 23/45 Exp 0] 0 msec 0 msec 0 msec
4 10.12.1.6 [MPLS: Labels 19/45 Exp 0] 4 msec 0 msec 0 msec
5 10.12.1.41 [MPLS: Label 45 Exp 0] 0 msec 4 msec 0 msec
6 10.12.1.42 0 msec 0 msec 0 msec
7 10.0.0.3 4 msec * 0 msec

```

If you select **(V)RF**, the AS is resolved in the VRF table, and the AS is indicated in the output of the command. For example:

Tracing the route to 10.0.0.3

```

1 10.1.1.9 [AS 100] [MPLS: Labels 25/45 Exp 0] 0 msec 4 msec 0 msec
2 10.1.1.1 [AS 100] [MPLS: Labels 26/45 Exp 0] 0 msec 0 msec 0 msec
3 10.12.1.101 [AS 100] [MPLS: Labels 23/45 Exp 0] 4 msec 0 msec 0 msec
4 10.12.1.6 [AS 100] [MPLS: Labels 19/45 Exp 0] 0 msec 4 msec 0 msec
5 10.12.1.41 [AS 100] [MPLS: Label 45 Exp 0] 0 msec 0 msec 4 msec
6 10.12.1.42 [AS 100] 0 msec 0 msec 0 msec
7 10.0.0.3 [AS 100] 0 msec * 0 msec

```

The path from a provider edge (PE)1 router to a PE2 router might contain routes from the global routing table and a VRF table. If that happens, you need to enter two interactive **traceroute vrf** commands at the PE1 router to trace the route to a customer edge (CE)2 router: one selecting the global routing table, and the other selecting a VRF table. You can then determine the valid and invalid AS numbers based on your knowledge of the network topology. In an interautonomous system (Inter-AS) network, however, you might not know the whole topology.

Common Traceroute Problems

Due to bugs in the IP implementation of various hosts and routers, the IP **traceroute** command might behave in an unexpected manner.

Not all destinations respond correctly to a probe message by sending back an “ICMP port unreachable” message. A long sequence of asterisks, terminating only when the maximum hop limit has been reached, might indicate this problem.

There is a known problem with the way some hosts handle an “ICMP TTL exceeded” message. Some hosts generate an “ICMP” message, but they reuse the Time to Live (TTL) of the incoming packet. Because the TTL of the incoming packet is 0, the Internet Control Message Protocol (ICMP) packets do not make it back. When you trace the path to such a host, you might see a set of TTL values with asterisks (*). Eventually the hop limit gets high enough that the “ICMP” message can get back. For example, if the host is six hops away, traceroute times out on responses 6 through 11.



Note

In IPv4, the TTL value can be an amount of time (for example, 250 milliseconds) or a hop count. In IPv6, the equivalent of the TTL value is always a hop count.

Examples

The following user EXEC example shows the IPv4 **traceroute** output that results when a destination host name has been specified:

```
Router> traceroute host77-name.domainZZ-name.com
```

Type escape sequence to abort.

Tracing the route to host77-name.domainZZ-name.com (10.0.0.73)

```

1 host1-name.domain1-name.com (192.168.1.6) 1000 msec 8 msec 4 msec
2 host33-name.serviceprovider8-name.com (192.168.16.2) 8 msec 8 msec 8 msec
3 host2-name.college2-name.edu (192.168.110.225) 8 msec 4 msec 4 msec

```

```

4 host44-name.domain2-name.NET (192.168.254.6) 8 msec 8 msec 8 msec
5 host22-name.serviceprovider99-name.com (192.168.3.8) 12 msec 12 msec 8 msec
6 host-name5.domain5-name.com (192.168.195.1) 216 msec 120 msec 132 msec
7 host77-name.domainZZ-name.com (10.0.0.73) 412 msec 628 msec 664 msec

```

Table 187 describes the significant fields shown in the display.

Table 187 *tracert Field Descriptions When IPv4 Is Used*

Field	Description
1	Indicates the sequence number of the router in the path to the host
host1-name.domain1-name.com	Host name of this router
192.168.1.6	Internet address of this router
1000 msec 8 msec 4 msec	Round-trip time for each of the three transmitted probes

The following user EXEC example shows the IPv6 **tracert** output that results when a destination host name has been specified:

```

Router> tracert host8-name.domainBB-name.no

Type escape sequence to abort.
Tracing the route to host8-name.domainBB-name.no (3FFE:2A00:100:7FF9::2)
 0 3FFE:C:00:E:13::2 28 msec 24 msec *
 1 3FFE:2A00:100:7FF8::2 208 msec 204 msec
 2 host32-name.domainHH-name.net (3FFE:2A00:100:7FF8::1) 276 msec * 276 msec
 3 host8-name.domainBB-name.no (3FFE:2A00:100:7FF9::2) 292 msec 292 msec 296 msec

```



Note

In the example, host8-name.domainBB-name.no has an IPv6 address, so the protocol for the **tracert** command defaults to IPv6. IPv4 could be used if you specify **ip** in the **tracert** command; for example, **tracert ip host8-name.domainBB-name.no**.

Table 188 describes the significant fields shown in the display.

Table 188 *tracert Field Descriptions When IPv6 Is Used*

Field	Description
4	Indicates the sequence number of the router in the path to the host
host8-name.domainBB-name.no	Host name of the destination node
3FFE:2A00:100:7FF9::2	IPv6 address of the destination node
292 msec 292 msec 296 msec	Round-trip time for each of the three transmitted probes

The following privileged EXEC example shows the extended dialog of the **tracert** command when IPv4 is used:

```

Router# tracert

Protocol [ip]:
Target IP address: host77-name.domainZZ-name.com
Source address:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:

```

```

Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to host77-name.domainZZ-name.com (10.0.0.73)
 0 host1-name.domain1-name.com (192.168.1.6) 1000 msec 8 msec 4 msec
 1 host33-name.serviceprovider8-name.com (192.168.16.2) 8 msec 8 msec 8 msec
 2 host2-name.college2-name.edu (192.168.110.225) 8 msec 4 msec 4 msec
 3 host44-name.domain2-name.NET (192.168.254.6) 8 msec 8 msec 8 msec
 4 host22-name.serviceprovider99-name.com (192.168.3.8) 12 msec 12 msec 8 msec
 5 host-name5.domain5-name.com (192.168.195.1) 216 msec 120 msec 132 msec
 6 host77-name.domainZZ-name.com (10.0.0.73) 412 msec 628 msec 664 msec

```

If an unknown host name is used in the Target IP address field, the software queries a Domain Name System (DNS) server to resolve the unknown host name to its IP address. In the following example, a DNS server (IP address 192.168.7.93) is queried for the unknown host name college9-name.edu:

```

Router# tracert

Protocol [ip]:
Target IP address: college9-name.edu
Translating "college9-name.edu"...domain server (192.168.7.93) [OK]

```

[Table 189](#) describes the fields that are unique to the extended traceroute sequence that is shown in the display.

Table 189 *tracert Field Descriptions When IPv4 Is Used*

Field	Description
Target IP address	You must enter an IPv4 host name or an IPv4 address. There is no default.
Source address	One of the interface addresses of the router to use as a source address for the probes. The router normally chooses what it considers to be the best source address.
Numeric display	The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display.
Timeout in seconds	The number of seconds to wait for a response to a probe packet. The default is 3 seconds.
Probe count	The number of probes to be sent at each TTL level. The default count is 3.
Minimum Time to Live [1]	The TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.
Maximum Time to Live [30]	The largest TTL value that can be used. The default is 30. The command terminates when the traceroute packet reaches the destination or when the value is reached.
Port Number	The destination port used by the User Datagram Protocol (UDP) probe messages. The default is 33434.
Loose, Strict, Record, Timestamp, Verbose	IP header options. You can specify any combination. The command issues prompts for the required fields. The command also places the requested options in each probe; however, there is no guarantee that all routers (or end nodes) will process the options.
Loose	Allows you to specify a list of nodes that the traceroute packet must traverse to the destination.

Table 189 *tracert Field Descriptions When IPv4 Is Used (continued)*

Field	Description
Strict	Allows you to specify a list of nodes that must be the only nodes traversed when the tracert packet goes to the destination.
Record	Allows you to specify the number of hops.
Timestamp	Allows you to specify the number of time stamps.
Verbose	If you select any option, the verbose mode is automatically selected, and the command prints the contents of the option field in any incoming packets. You can prevent verbose mode by selecting it again and toggling its current setting.

The following privileged EXEC example shows the extended dialog of the **tracert** command when IPv6 is used:

```
Router# tracert

Protocol [ip]: ipv6
Target IP address: host8-name.domainBB-name.no
Source IPv6 address:
Numeric display [no]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Priority [0]:
Port Number [33434]:
Type escape sequence to abort.
Tracing the route to host8-name.domainBB-name.no (3FFE:2A00:100:7FF9::2)
 1 3FFE:C:00:E:13::2 28 msec 24 msec *
 2 3FFE:2A00:100:7FF8::2 208 msec 204 msec
 3 host32-name.domainHH-name.net (3FFE:2A00:100:7FF8::1) 276 msec * 276 msec
 4 host8-name.domainBB-name.no (3FFE:2A00:100:7FF9::2) 292 msec 292 msec 296 msec
```

If an unknown host name is used in the Target IP address field, software queries a DNS server to resolve the unknown host name to an IP address. In the following example, a DNS server (IP address 192.168.7.93) is queried for the unknown host name host8-name.domainBB-name.no:

```
Router# tracert

Protocol [ip]: ipv6
Target IP address: host8-name.domainBB-name.no
Translating "host8-name.domainBB-name.no"...domain server (192.168.7.93) [OK]
```

[Table 190](#) describes the fields that are unique to the extended **tracert** sequence shown in the display.

Table 190 *tracert Field Descriptions When IPv6 Is Used*

Field	Description
Protocol [ip]:	The protocol to use for the probes. The available protocols are appletalk , clns , ip , ipv6 , ipx , oldvines , and vines . The default is ip .
Target IP address	You must enter an IPv6 host name or an IPv6 address. There is no default.

Table 190 *tracertool Field Descriptions When IPv6 Is Used (continued)*

Field	Description
Source IPv6 address	The IPv6 address of an interface in the router that is used as the source address for the probes. If you do not enter an address, the router chooses what it considers to be the best source address. Note In Cisco IOS Release 12.2(8)T and later releases, an IPv6 address enclosed in square brackets ([]), such as [FE80::260:3EFF:FE11:6770], is acceptable to the system. Refer to RFC 2732, <i>Format for Literal IPv6 Addresses in URL's</i> , for more information on the use of square brackets with literal IPv6 addresses as in URLs.
Numeric display	The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display.
Timeout in seconds	The number of seconds to wait for a response to a probe packet. The default is 3 seconds.
Probe count	The number of probes to be sent at each TTL level. The default count is 3.
Minimum Time to Live [1]	The HopCount (TTL) value or hop limit for the first probes. The default is 1, but it can be set to a higher value if you want to suppress the display of known hops.
Maximum Time to Live [30]	The largest HopCount (TTL) value or hop limit that can be used. The default is 30. The command terminates when the tracertool packet reaches the destination or when this value is reached.
Port Number	The destination port used by the UDP probe messages. The default is 33434.

[Table 191](#) describes the characters that can appear in **tracertool** command output when IPv4 is used.

Table 191 *tracertool Text Characters When IPv4 Is Used*

Character	Description
nn msec	For each node, the round-trip time (in milliseconds) for the specified number of probes.
*	The probe timed out. No response was received within the specified period.
?	Unknown error.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable (beyond scope).
P	Protocol unreachable.
Q	Source quench.
P	Port unreachable.

[Table 192](#) describes the characters that can appear in the **tracertool** command output when IPv6 is used.

Table 192 *tracertool Text Characters When IPv6 Is Used*

Character	Description
!	Indicates receipt of a reply.
*	The probe timed out. No response was received within the specified period.
?	Unknown error.
@	Unreachable for unknown reason.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable (beyond scope).
P	Port unreachable.
U	No route to host.

transfer-interval

To configure how long bulk statistics should be collected before a bulk statistics transfer is initiated, use the **transfer-interval** command in Bulk Statistics Transfer configuration mode. To remove a previously configured interval from a bulk statistics configuration, use the **no** form of this command.

transfer-interval *minutes*

no transfer-interval *minutes*

Syntax Description	<i>minutes</i>	Length of time, in minutes, that the system should collect MIB data before attempting the transfer operation. The valid range is from 1 to 2147483647. The default is 30 minutes.
---------------------------	----------------	---

Defaults Bulk statistics file transfer operations start 30 minutes after the **enable** (bulkstat) command is used.

Command Modes Bulk Statistics Transfer configuration (config-bulk-tr)

Command History	Release	Modification
	12.0(24)S	This command was introduced.
	12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines Because bulk statistics data is collected into a new file once a transfer attempt begins, this command also configures the collection interval.

If the maximum buffer size for a bulk statistics file is reached before the transfer interval time expires, the transfer operation will still be initiated, and bulk statistics MIB data will be collected into a new file in the system buffer.

Examples The following example configures the transfer interval for the bulk statistics configuration bulkstat1 to 20 minutes:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# transfer-interval 20
```

Related Commands	Command	Description
	snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.

transport event

To specify that inventory events are sent out by the CNS inventory agent, use the **transport event** command in CNS inventory configuration mode. To disable the transport of inventory events, use the **no** form of this command.

transport event

no transport event

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes CNS inventory configuration

Command History	Release	Modification
	12.3(1)	This command was introduced.

Usage Guidelines Use this command to send out inventory requests with each CNS inventory agent message. When configured, the routing device will respond to queries from the CNS Event Bus. Online insertion and removal (OIR) events on the routing device will be reported to the CNS Event Bus.

Examples The following example shows how to enable the CNS inventory agent and configure it to send out inventory events:

```
Router(config)# cns inventory
Router(cns_inv)# transport event
```

Related Commands	Command	Description
	cns inventory	Enables the CNS inventory agent and enters CNS inventory configuration mode.

ttl dns

To configure the number of seconds for which an answer received from the boomerang client will be cached by the Domain Name System (DNS) client, use the **ttl dns** command in boomerang configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

ttl dns *seconds*

no ttl dns *seconds*

Syntax Description	<i>seconds</i>	Number of seconds for which an answer received from the boomerang client will be cached by the DNS client. Range is from 10 to 2147483647.
---------------------------	----------------	--

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	Boomerang configuration
----------------------	-------------------------

Command History	Release	Modification
	12.2(8)T	This command was introduced.

Usage Guidelines	<p>The ttl dns command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the DRP agent.</p> <p>The ttl dns command configures the number of seconds for which the DNS client can cache a boomerang reply from a boomerang client.</p>
-------------------------	---

Examples	In the following example, the number of seconds for which the DNS client can cache a boomerang reply from a boomerang client is configured as 10:
-----------------	---

```
Router(config)# ip drp domain www.boom1.com
Router(config-boomerang)# ttl dns 10

Router# show running-config
.
.
.
ip drp domain www.boom1.com
dns-ttl 10
```

Related Commands

Command	Description
alias (boomerang configuration)	Configures an alias name for a specified domain.
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.
server (boomerang configuration)	Configures the server address for a specified boomerang domain.
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttd ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

ttl ip

To configure the IP time-to-live (TTL) value for the boomerang response packets sent from the boomerang client to the DNS client, use the **ttl ip** command in boomerang configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

ttl ip *hops*

no ttl ip *hops*

Syntax Description	<i>hops</i>	Number of hops that occur between the boomerang client and the DNS client before the boomerang response packet fails. Range is from 1 to 255.
---------------------------	-------------	---

Defaults No default behavior or values.

Command Modes Boomerang configuration

Command History	Release	Modification
	12.2(8)T	This command was introduced.

Usage Guidelines The **ttl ip** command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the DRP agent.

The **ttl ip** command configures the maximum number of hops allowed between the boomerang client and the DNS client, after which the boomerang response packet fails. If the user wants to restrict the contending proxies only to nearby ones, the value of the **ttl ip** command can be set to a specific number within the allowed range. Any proxy outside of this range will be automatically disqualified in the boomerang race because its replies will never reach the DNS client. Because the **ttl ip** command specifies the number of hops for which a response from a client will live, it allows faraway proxies to avoid wasting bandwidth.

Examples In the following example, the number of hops that occur between the boomerang client and the DNS client before the boomerang response packet fails is configured as 2:

```
Router(config)# ip drp domain www.boom1.com
Router(config-boomerang)# ttl ip 2

Router# show running-config
.
.
.
ip drp domain www.boom1.com
ip-ttl 2
```

Related Commands

Command	Description
alias (boomerang)	Configures an alias name for a specified domain.
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.
server (boomerang)	Configures the server address for a specified boomerang domain.
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttl dns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.