databits

To set the number of data bits per character that are interpreted and generated by the router hardware, use the **databits** command in line configuration mode. To restore the default value, use the **no** form of the command.

databits {**5** | **6** | **7** | **8**}

no databits

Syntax Description

5	Five 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

Eight data bits per character

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **databits** line configuration 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 are supplied for compatibility with older devices and generally are not used.

Examples

The following example sets the number of data bits per character to seven on line 4:

```
Router(config)# line 4
Router(config-line)# databits 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 databits	Changes the number of data bits per character for the current terminal line for this session.
terminal data-character-bits	Sets the number of data bits per character that are interpreted and generated by the Cisco IOS software for the current line and session.

data-character-bits

To set the number of data bits per character that are interpreted and generated by the Cisco IOS software, use the **data-character-bits** command in line configuration mode. To restore the default value, use the **no** form of this command.

data-character-bits {**7** | **8**}

no data-character-bits

Syntax Description

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

Defaults

Eight data bits per character

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

Examples

The following example sets the number of data bits per character to seven on virtual terminal line (vty) 1:

```
Router(config)# line vty 1
Router(config-line)# data-character-bits 7
```

Related Commands

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

default-value data-character-bits

To configure the number of data bits per character that are generated and interpreted by Cisco software to either 7 bits or 8 bits, use the **default-value data-character-bits** command in global configuration mode. To disable the configured size, use the **no** form of this command.

default-value data-character-bits {**7** | **8**}

no default-value data-character-bits

Syntax Description

7	Selects 7 bits as the default size.
8	Selects 8 bits as the default size.

Command Default

8 data bits per character are generated.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRB	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows how to set the default number of data character bits to 8:

```
Router# configure terminal
Router(config)# default-value data-character-bits 8
```

Related Commands

Command	Description
default-value exec-character-bits	Defines the EXEC character width to either 7 bits or 8 bits.
default-value modem-signal	Configures the default frequency time to scan modem signals.
default-value special-character-bits	Configures the flow control default value from a 7-bit width to an 8-bit width.

default-value exec-character-bits

To define the EXEC character width for either 7 bits or 8 bits, use the **default-value exec-character-bits** command in global configuration mode. To restore the default value, use the **no** form of this command.

default-value exec-character-bits {**7** | **8**}

no default-value exec-character-bits

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

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Configuring the EXEC character width to 8 bits allows you to add graphical and international characters in banners, prompts, and so on. However, setting the EXEC character width to 8 bits can also cause failures. 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, although the eighth bit is not needed for the **help** command.

Examples

The following example selects the full 8-bit ASCII character set for EXEC banners and prompts:

```
Router(config)# default-value exec-character-bits 8
```

Related Commands

Command	Description
default-value special-character-bits	Configures the flow control default value from a 7-bit width to an 8-bit width.
exec-character-bits	Configures the character widths of EXEC and configuration command characters.
length	Sets the terminal screen length.
terminal exec-character-bits	Locally changes the ASCII character set used in EXEC and configuration command characters for the current session.
terminal special-character-bits	Changes the ASCII character widths to accept special characters for the current terminal line and session.

default-value modem-interval

To configure the default frequency time to scan modem signals, use the **default-value modem-interval** command in global configuration mode. To disable the configured frequency, use the **no** form of this command.

default-value modem-interval *milliseconds*

no default-value modem-interval

Syntax Description

milliseconds	Time frequency, in milliseconds (ms). The range is from 0 to 1000.

Command Default

The frequency time to scan modem signals is 50 ms.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to set the default time to scan the modem signal to 345 ms:

```
Router# configure terminal
Router(config)# default-value modem-signal 345
```

Related Commands

Command	Description
default-value data-character-bits	Configures the default size of bits handled to either 7 bits or 8 bits.
default-value exec-character-bits	Defines the EXEC character width to either 7 bits or 8 bits.
default-value special-character-bits	Configures the flow control default value from a 7-bit width to an 8-bit width.

default-value special-character-bits

To configure the flow control default value from a 7-bit width to an 8-bit width, use the **default-value special-character-bits** command in global configuration mode. To restore the default value, use the **no** form of this command.

default-value special-character-bits {**7** | **8**}

no default-value special-character-bits

Syntax Description

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

Defaults

7-bit character set

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Configuring the special character width to 8 bits allows you to add graphical and international characters in banners, prompts, and so on.

Examples

The following example selects the full 8-bit special character set:

```
Router(config)# default-value special-character-bits 8
```

Related Commands

Command	Description
default-value exec-character-bits	Defines the EXEC character width for either 7 bits or 8 bits.
exec-character-bits	Configures the character widths of EXEC and configuration command characters.
length	Sets the terminal screen length.
terminal exec-character-bits	Locally changes the ASCII character set used in EXEC and configuration command characters for the current session.
terminal special-character-bits	Changes the ASCII character widths to accept special characters for the current terminal line and session.

define interface-range

To create an interface-range macro, use the **define interface-range** command in global configuration mode.

define interface-range *macro-name interface-range*

Syntax Description

macro-name	Name of the interface range macro; the macro name can contain up to 32 characters.
interface-range	Interface range. For a list of valid values for interface ranges, see the "Usage Guidelines" section.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The macro name is a 32-character maximum character string.

Amn interface range for a macro can contain up to five ranges. An interface range cannot span slots. Use this format when entering the *interface-range*:

- *interface-type slot/first-interface - last-interface*

Valid values for *card-type* are as follows:

- **ethernet**
- **fastethernet**
- **gigabitethernet**
- loopback
- **tengigabitethernet**
- **tunnel**
- **vlan** *vlan-id* (valid values are from 1 to 4094)
- **port-channel** *interface-number* (valid values are from 1 to 256)
- **ge-wan**—supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2
- **pos**—supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2
- **atm**—supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2

Examples

This example shows how to create a multiple-interface macro:

```
Router(config)# define interface-range macro1 ethernet 1/2 - 5, fastethernet 5/5 - 10
Router(config)#
```

Related Commands

Command	Description
interface range	Executes a command on multiple ports at the same time.

delete

To delete a file on a Flash memory device or NVRAM, use the **delete** command in EXEC, privileged EXEC, or diagnostic mode.

delete *url* [**/force** | **/recursive**]

Syntax Description

url	Cisco IOS File System URL of the file to be deleted. Include the file system prefix, followed by a colon, and, optionally, the name of a file or directory. See Table 27 for list of supported URLs.
/force	(Optional) Deletes the specified file or directory without prompting you for verification. **Note** Use this keyword with caution: the system will not ask you to confirm the file deletion.
/recursive	(Optional) Deletes all files in the specified directory, as well as the directory itself.

Command Modes

EXEC (>)

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
11.0	This command was introduced.
12.3(14)T	The **usbflash**[**0**-**9**]**:** and **usbtoken**[**0**-**9**]**:** options were added to the list of Cisco IOS File System URLs.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers and the following enhancements were introduced: • This command was introduced in diagnostic mode for the first time. The command can be entered in both privileged EXEC and diagnostic mode on the Cisco ASR1000 Series Routers. • The **harddisk:**, **obfl:**, **stby-bootflash:**, **stby-harddisk:**, **stby-nvram:**, **stby-obfl:**, **stby-usb**[**0**-**1**]**:**, and **usb**[**0**-**1**]**:** *url* options were introduced.

Usage Guidelines

If you attempt to delete the configuration file or image specified by the CONFIG_FILE or BOOTLDR environment variable, the system prompts you to confirm the deletion. Also, if you attempt to delete the last valid system image specified in the BOOT environment variable, the system prompts you to confirm the deletion.

When you delete a file in Flash memory, the software simply marks the file as deleted, but it does not erase the file. To later recover a “deleted” file in Flash memory, use the **undelete** EXEC command. You can delete and undelete a file up to 15 times.

To permanently delete all files marked “deleted” on a linear Flash memory device, use the **squeeze** EXEC command.

Table 27 contains a list of Cisco IOS File System URLs.

Table 27 URL File System Prefix Keywords

Prefix	Filesystem
bootflash:	Delete the file from boot Flash memory.
flash:	Delete the file from Flash memory.
harddisk:	Delete the file from the harddisk file system.
nvram:	Delete the from the router NVRAM.
obfl:	Delete the file from the onboard failure logging file system.
slot0:	Delete the file from the first PCMCIA Flash memory card.
stby-bootflash:	Delete the file from the standby bootflash file system.
stby-harddisk:	Delete the file from the standby harddisk file system.
stby-nvram:	Delete the from the router NVRAM on the standby hardware.
stby-obfl:	Delete the file from the onboard failure logging file system on the standby hardware.
stby-usb[**0**-**1**]:	Delete the file from the standby USB Flash drive.
usb[**0**-**1**];	Delete the file from the USB Flash drive.
usbflash[**0**-**9**]**:**	Delete the file from the USB Flash drive.
usbtoken[**0**-**9**]**:**	Delete the file from the USB eToken.

Examples

The following example deletes the file named test from the Flash card inserted in slot 0:

```
Router# delete slot0:test
Delete slot0:test? [confirm]
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
squeeze	Permanently deletes Flash files by squeezing a Class A Flash file system.
undelete	Recovers a file marked “deleted” on a Class A or Class B Flash file system.

diag

To perform field diagnostics on a line card, on the Gigabit Route Processor (GRP), on the Switch Fabric Cards (SFCs), and on the Clock Scheduler Card (CSC) in Cisco 12000 series Gigabit Switch Routers (GSRs), use the **diag** command in privileged EXEC mode. To disable field diagnostics on a line card, use the **no** form of this command.

diag *slot-number* [**halt** | **previous** | **post** | **verbose** [**wait**] | **wait**]

no diag *slot-number*

Syntax Description

slot-number	Slot number of the line card you want to test. Slot numbers range from 0 to 11 for the Cisco 12012 and 0 to 7 for the Cisco 12008 router. Slot numbers for the CSC are 16 and 17, and for the FSC are 18, 19, and 20.
halt	(Optional) Stops the field diagnostic testing on the line card.
previous	(Optional) Displays previous test results (if any) for the line card.
post	(Optional) Initiates an EPROM-based extended power-on self-test (EPOST) only. The EPOST test suite is not as comprehensive as the field diagnostics, and a pass/fail message is the only message displayed on the console.
verbose [**wait**]	(Optional) Enables the maximum status messages to be displayed on the console. By default, only the minimum status messages are displayed on the console. If you specify the optional **wait** keyword, the Cisco IOS software is not automatically reloaded on the line card after the test completes.
wait	(Optional) Stops the automatic reloading of the Cisco IOS software on the line card after the completion of the field diagnostic testing. If you use this keyword, you must use the **microcode reload** *slot* global configuration command, or manually remove and insert the line card (to power it up) in the slot so that the GRP will recognize the line card and download the Cisco IOS software image to the line card.

Defaults

No field diagnostics tests are performed on the line card.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12000 series GSR.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **diag** command must be executed from the GRP main console port.

Perform diagnostics on the CSC only if a redundant CSC is in the router.

Diagnostics will stop and ask you for confirmation before altering the router's configuration. For example, running diagnostics on a SFC or CSC will cause the fabric to go from full bandwidth to one-fourth bandwidth. Bandwidth is not affected by GRP or line card diagnostics.

The field diagnostic software image is bundled with the Cisco IOS software and is downloaded automatically from the GRP to the target line card prior to testing.

Caution Performing field diagnostics on a line card stops all activity on the line card. Before the **diag** EXEC command begins running diagnostics, you are prompted to confirm the request to perform field diagnostics on the line card.

In normal mode, if a test fails, the title of the failed test is displayed on the console. However, not all tests that are performed are displayed. To view all the tests that are performed, use the **verbose** keyword.

After all diagnostic tests are completed on the line card, a PASSED or TEST FAILURE message is displayed. If the line card sends a PASSED message, the Cisco IOS software image on the line card is automatically reloaded unless the **wait** keyword is specified. If the line card sends a TEST FAILURE message, the Cisco IOS software image on the line card is not automatically reloaded.

If you want to reload the line card after it fails diagnostic testing, use the **microcode reload** *slot* global configuration command.

Note When you stop the field diagnostic test, the line card remains down (that is, in an unbooted state). In most cases, you stopped the testing because you need to remove the line card or replace the line card. If that is not the case, and you want to bring the line card back up (that is, online), you must use the **microcode reload** global configuration command or power cycle the line card.

If the line card fails the test, the line card is defective and should be replaced. In future releases this might not be the case because DRAM and SDRAM SIMM modules might be field replaceable units. For example, if the DRAM test failed you might only need to replace the DRAM on the line card.

For more information, refer to the Cisco 12000 series installation and configuration guides.

Examples

In the following example, a user is shown the output when field diagnostics are performed on the line card in slot 3. After the line card passes all field diagnostic tests, the Cisco IOS software is automatically reloaded on the card. Before starting the diagnostic tests, you must confirm the request to perform these tests on the line card because all activity on the line card is halted. The total/indiv. timeout set to 600/220 sec. message indicates that 600 seconds are allowed to perform all field diagnostics tests, and that no single test should exceed 220 seconds to complete.

```
Router# diag 3

Running Diags will halt ALL activity on the requested slot. [confirm]
Router#
Launching a Field Diagnostic for slot 3
Running DIAG config check
RUNNING DIAG download to slot 3 (timeout set to 400 sec.)
sending cmd FDIAG-DO ALL to fdiag in slot 3
(total/indiv. timeout set to 600/220 sec.)
Field Diagnostic ****PASSED**** for slot 3


Field Diag eeprom values: run 159 fial mode 0 (PASS) slot 3
   last test failed was 0, error code 0
```

```
sending SHUTDOWN FDIAG_QUIT to fdiag in slot 3

Board will reload
.
.
.
Router#
```

In the following example, a user is shown the output when field diagnostics are performed on the line card in slot 3 in verbose mode:

```
Router# diag 3 verbose

Running Diags will halt ALL activity on the requested slot. [confirm]
Router#
Launching a Field Diagnostic for slot 3
Running DIAG config check
RUNNING DIAG download to slot 3 (timeout set to 400 sec.)
sending cmd FDIAG-DO ALL to fdiag in slot 3
(total/indiv. timeout set to 600/220 sec.)
FDIAG_STAT_IN_PROGRESS: test #1 R5K Internal Cache
FDIAG_STAT_PASS test_num 1
FDIAG_STAT_IN_PROGRESS: test #2 Sunblock Ordering
FDIAG_STAT_PASS test_num 2
FDIAG_STAT_IN_PROGRESS: test #3 Dram Datapins
FDIAG_STAT_PASS test_num 3
.
.
.
Field Diags: FDIAG_STAT_DONE
Field Diagnostic ****PASSED**** for slot 3
Field Diag eeprom values: run 159 fial mode 0 (PASS) slot 3
   last test failed was 0, error code 0
sending SHUTDOWN FDIAG_QUIT to fdiag in slot 3

Board will reload
.
.
.
Router#
```

Related Commands

Command	Description
microcode reload	Reloads the Cisco IOS image on a line card on the Cisco 7000 series with RSP7000, Cisco 7500 series, or Cisco 12000 series routers after all microcode configuration commands have been entered.

diagnostic bootup level

To set the diagnostic bootup level, use the **diagnostic bootup level** command in global configuration mode. To skip all diagnostic tests, use the **no** form of this command.

diagnostic bootup level {**minimal** | **complete**}

no diagnostic bootup level

Syntax Description

minimal	Specifies minimal diagnostics. See the Usage Guidelines section for additional information.
complete	Specifies complete diagnostics. See the Usage Guidelines section for additional information.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCC	The command was integrated in this release to support Generic Online Diagnostics (GOLD) functionality for Cisco UBR10012 Universal Broadband Router.

Usage Guidelines

Setting the diagnostic level determines the level of testing that occurs when the system or module is reset. The two levels are as follows:

- Complete—Runs all tests.
- Minimal—Runs only EARL tests for the supervisor engine and loopback tests for all ports in the system.

Note Although the default is **minimal**, you can set the diagnostic level to **complete** for troubleshooting hardware problems.

In certain circumstances, you might want to skip the bootup online diagnostics completely. For example, you might skip the bootup online diagnostics to verify that a port is as bad as online diagnostics reports. To skip online diagnostic testing completely, use the **no diagnostic bootup level** command.

For information on the diagnostic test types, use the **show diagnostic** command.

The new level takes effect at the next reload or the next time that an online insertion and removal is performed.

Examples

The following example shows how to set the diagnostic bootup level:

```
Router(config)# diagnostic bootup level complete
```

Related Commands

Command	Description
show diagnostic bootup level	Displays the coverage level for the configured bootup diagnostics.

diagnostic cns

To configure the Cisco Networking Services (CNS) diagnostics, use the **diagnostic cns** command in global configuration mode. To disable sending diagnostic results to the CNS event bus., use the **no** form of this command.

diagnostic cns {**publish** | **subscribe**} [*subject*]

no diagnostic cns {**publish** | **subscribe**} [*subject*]

Syntax Description

publish	Sends diagnostic results to a remote network application to make decisions and take corrective actions that are based on the diagnostic results.
subscribe	Receives messages from remote network applications to perform diagnostic tests or retrieve diagnostic results.
subject	(Optional) Event subject name.

Defaults

The following are the default settings for **diagnostic cns**:

diagnostic cns publish cisco.cns.device.diag_results

diagnostic cns subscribe cisco.cns.device.diag_commands

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The online diagnostics receive events by subscribing to an event *subject* name. The *subject* is the event that you subscribe (receive) or publish (generate) through the CNS bus.

The **diagnostic cns publish** command sends diagnostic results to a remote network application to make decisions and take corrective actions that are based on the diagnostic results.

The **diagnostic cns subscribe** command receives messages from remote network applications to perform diagnostic tests or retrieve diagnostic results.

Examples

This example shows how to enable the publishing of diagnostic results:

```
Router(config)# diagnostic cns publish my.cns.publish
Router(config)#
```

This example shows how to receive messages from remote network applications to perform diagnostic tests or retrieve diagnostic results:

```
Router(config)# diagnostic cns subscribe my.cns.subscribe
Router(config)#
```

This example shows how to set the default to **publish**:

```
Router(config)# default diagnostic cns publish
Router(config)#
```

Related Commands

Command	Description
show diagnostic cns publish	Displays the publish information about the CNS subject.
show diagnostic cns subscribe	Displays the subscribe information about the CNS subject.

diagnostic event-log size

To modify the diagnostic event log size dynamically, use the **diagnostic event-log size** command in global configuration mode. To return to the default settings, use the **no** form of this command.

diagnostic event-log size *size*

no diagnostic event-log size

Syntax Description

size	Diagnostic event-log sizes. The valid values range from 1 to 10000 entries.

Command Default

The event log size is **500** entries.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA.	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCC	The command was integrated in this release to support Generic Online Diagnostics (GOLD) functionality for Cisco UBR10012 Universal Broadband Router.

Usage Guidelines

The events are dynamically allocated and stored in a circular queue.

You can enter either the **default diagnostic event-log size** command or the **no diagnostic event-log size** command to return to the default settings.

Examples

The following example shows how to set the diagnostic event-log size:

```
Router(config)# diagnostic event-log size 600
```

Related Commands

Command	Description
show diagnostic events	Displays the event log for the diagnostic events.

diagnostic level

To turn on power-on diagnostic tests for the network service engines (NSEs) installed in a Cisco 7300 series router, use the **diagnostic level** command in privileged EXEC configuration mode. There is no **no** form of this command.

diagnostic level {**power-on** | **bypass**}

Syntax Description

power-on	Power-on diagnostic tests are performed at system bootup on the NSEs.
bypass	No diagnostic tests are performed. This is the default.

Defaults

No diagnostic tests are performed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EX2	This command was introduced.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2 S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to enable power-on diagnostic tests to run on the installed NSEs of a Cisco 7300 series router when the system is booted. It is recommended that you issue this command only if you are experiencing problems with an NSE and are planning on rebooting the router. Issuing this command causes an increase in the boot time.

Examples

The following example shows how to enable diagnostic power-on tests:

```
diagnostic level power-on
```

The following sample output shows the output that is displayed upon system bootup after a power cycle or router crash:

```
.
.
.
System Power On Diagnostics
DRAM Size .....................128 MB
Testing DRAM...................Passed
Level2 Cache ..................Present
Testing Level2 Cache (256  KB)Passed
Level3 Cache ..................Present
```

```
Testing Level3 Cache (1024 KB)Passed

System Power On Diagnostics Complete
```

Note This output is displayed when the system is booting, not when the command is issued.

Related Commands

Command	Description
debug redundancy	Enables NSE redundancy debugging.
show c7300	Displays the types of cards (NSE and line cards) installed in a Cisco 7300 series router.
show redundancy (7300)	Displays redundancy information for the active and standby NSEs.

diagnostic monitor

To configure health-monitoring diagnostic testing, use the **diagnostic monitor** command in global configuration mode. To disable testing, use the **no** form of this command.

diagnostic monitor interval module *number* **test** {*test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds days*

diagnostic monitor syslog

diagnostic monitor module *num* **test** {*test-id* | *test-id-range* | **all**}

no diagnostic monitor {**interval** | **syslog**}

Cisco UBR10012 Router

diagnostic monitor {**bay** *slot/bay* | **slot** *slot number* | **subslot** *slot/subslot*} **test** {*test-id* | *test-id-range* | **all**}

diagnostic monitor interval {**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/subslot*} **test** {*test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds days*

diagnostic monitor syslog

diagnostic monitor threshold {**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/subslot*} **test** {*test-id* | *test-id-range* | **all**} {**failure count** *failures*} [{**runs** | **days** | **hours** | **minutes** | **seconds** | **milliseconds**} *window_size*]

Syntax Description

interval	Sets the interval between testing.
module *number*	Specifies the module number.
test	Specifies a test to run.
test-id	Identification number for the test to run. See the “Usage Guidelines” section for additional information.
test-id-range	Range of identification numbers for tests to be run. See the “Usage Guidelines” section for additional information.
all	Runs all the diagnostic tests.
hour *hh*	(Optional) Specifies the number of hours between tests. See the “Usage Guidelines” section for formatting guidelines.
min *mm*	(Optional) Specifies the number of minutes between tests. See the “Usage Guidelines” section for formatting guidelines.
second *ss*	(Optional) Specifies the number of seconds between tests. See the “Usage Guidelines” section for formatting guidelines.
millisec *ms*	(Optional) Specifies the number of milliseconds between tests; see the “Usage Guidelines” section for formatting guidelines.
syslog	Enables system logging messages when a health-monitoring test fails.
bay *slot/bay*	Indicates the card slot and bay number where the diagnostic test is run periodically and monitored. The **bay** keyword is used to refer a SPA on the router. The valid range for the slot number is from 1 to 8 and 0 to 3 for the bay number.

slot *slotnumber*	Indicates the slot number of the full-height line card where the diagnostic test is run periodically and monitored. The **slot** keyword is used to refer a full-height line card on the router. The valid range for the slot is from 1 to 8.
subslot *slot/subslot*	Indicates the slot and subslot number of half-height line card on which the diagnostic test is run periodically and monitored. The **subslot** keyword is used to refer a half-height line card on the router. The valid range for the slot number is from 1 to 8 and 0 to 1 for the subslot number.
threshold	Configures the failure threshold value for the specified bay, slot, or subslot.
failure count *failures*	Configures the count for maximum failures allowed after which the failed test results are displayed in the output of the **show diagnostic results** command. The range for number of allowed failures is 0 to 99.
hh:mm:ss	Hours, minutes, and seconds interval configured to run the test again.
milliseconds	Number of milliseconds between tests.
days	Number of days between tests. The valid range is from 0 to 20.
runs *window_size*	Number of test-run count for the failure window-size.
days *window_size*	Number of days for the failure window-size.
hours *window_size*	Number of hours for the failure window-size.
minutes *window_size*	Number of minutes for the failure window-size.
seconds *window_size*	Number of seconds for the failure window-size.
milliseconds *window_size*	Number of milliseconds for the failure window-size.

Command Default

The defaults are as follows:

- Depending on the test run, monitoring may be enabled or disabled.
- Depending on the test run, the default monitoring interval varies.
- **syslog** is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCC	The command was integrated into Cisco IOS Release 12.2(33)SCC to support Generic Online Diagnostics (GOLD) functionality for Cisco UBR10012 Universal Broadband Router. The keywords **bay**, **slot**, and **subslot** were added for the Cisco UBR10012 Universal Broadband Router.

Usage Guidelines

Use these guidelines when scheduling testing:

- *test-id*—Enter the **show diagnostic content** command to display the test ID list.
- *test-id-range*—Enter the **show diagnostic content** command to display the test ID list. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).
- *hh*—Enter the hours from 1 to 24.
- *mm*—Enter the minutes from 1 to 60.
- *days*—Enter the number of days between tests.
- *ss*—Enter the seconds from 1 to 60.
- *ms*—Enter the milliseconds from 1 to 1000.

Enter the [**no**] **diagnostic monitor test** {*test-id* | *test-id-range* | **all**} command to enable or disable the specified health monitoring test.

When entering the **diagnostic monitor module** *number* **test** {*test-id* | *test-id-range* | **all**} command, observe the following:

- Required
  - Isolate network traffic by disabling all connected ports and do not pump test packets during the test.
  - Remove all modules for testing FIB TCAM and SSRAM memory on the PFC of the supervisor engine.
  - Reset the system or the test module before putting the system back into the normal operating mode.
- Recommended
  - If the DFC module is present, remove all modules, and then reboot the system before starting the memory test on the central PFC3B of the supervisor engine.
  - Turn off all background health-monitoring tests on the supervisor engine and the modules using the **no diagnostic monitor module** *number* **test** {*test-id* | *test-id-range* | **all**} command.

The FIB TCAM test for central PFC3BXL or PFC3B (on the supervisor engine) takes approximately 4 hours and 30 minutes.

The FIB TCAM test for the distributed PFC3BXL or PFC3B (on the DFC module) takes approximately 16 hours.

You can run the FIB TCAM test on multiple DFC3BX modules simultaneously.

Cisco UBR10012 Router

The command syntax to refer a line card or SPAs is different on Cisco UBR10012 Router. The keyword is **slot x** for a full-height line card, **slot x/y** for a half-height card, and **bay x/y** for a SPA.

To monitor a diagnostic test periodically, you first need to configure the hours, minutes, and seconds interval to run the diagnostic test using the **diagnostic monitor interval** command. An error message is displayed, if the interval is not configured before enabling the monitoring.

To store log details for failed tests, execute the **diagnostic monitor syslog** command. A threshold value to specify the maximum count for allowed failures is configured using the **diagnostic monitor threshold** command. The failed test results can be viewed using the **show diagnostic results** command, after the number of failed test reaches the maximum number of allowed failures configured using the **diagnostic monitor threshold** command.

Examples

The following example shows how to run the specified test every 3 days:

```
Router(config)# diagnostic monitor interval module 5 test 7 09:07:05 45 3
```

The following example shows how to enable the generation of a syslog message when any health-monitoring test fails:

```
Router(config)# diagnostic monitor syslog
```

Cisco UBR10012 Router

The following example shows a sample output of an error message displayed when monitoring is enabled before configuring the test interval:

```
Router(config)# diagnostic monitor bay 1/0 test 2
Aug 12 18:04:56.280: %DIAG-3-MONITOR_INTERVAL_ZERO: Bay 1/0: Monitoring interval
 is 0. Cannot enable monitoring for Test #2
```

The following example shows how to configure the periodic interval for running diagnostic tests on the the router before enabling monitoring:

```
Router(config)# diagnostic monitor interval bay 1/0 test 2 06:00:00 100 10
```

The following example shows how to enable the diagnostic monitoring on bay 1/0:

```
Router(config)# diangostic monitor bay 1/0 test 2
```

The following example shows how to enable logging of failed messages to syslog:

```
Router(config)# diangostic monitor syslog
```

The following example shows how to configure the failure threshold value after which the failed test results are displayed in the command output for **show diagnostic results**:

```
Router(config)# diagnostic monitor threshold bay 1/0 test 2 failure count 10
```

Related Commands

Command	Description
show diagnostic content	Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all modules.

diagnostic ondemand

To configure the on-demand diagnostics, use the **diagnostic ondemand** command in privileged EXEC mode.

diagnostic ondemand {**iteration** *iteration-count* | **action-on-failure** {**continue** *error-count* | **stop**}}

Syntax Description

iteration *iteration-count*	Sets the number of times the same test to rerun when the command is issued. The valid range for iteration-count is between 1 to 999.
action-on-failure	Sets the execution action when a failure is detected.
continue	Continues testing when a test failure is detected.
stop	Stops testing when a test failure is detected.
error-count	(Optional) Number of errors that are allowed before stopping. This argument is used with the **continue** option. The valid range for error-count is from 0 to 65534.

Command Default

The default settings are as follows:

- *iteration-count* is **1**.
- **action-on-error** is **continue**.
- *error-count* is **0**.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCC	The command was integrated in this release to support Generic Online Diagnostics (GOLD) functionality for Cisco UBR10012 Universal Broadband Router.

Usage Guidelines

Entering **0** for the *error-count* sets the number of errors that are allowed to unlimited.

Examples

The following example shows how to set the ondemand testing iteration count:

```
Router# diagnostic ondemand iteration 4
Router#
```

The following example shows how to set the execution action when an error is detected:

```
Router# diagnostic ondemand action-on-failure continue 2
Router#
```

Related Commands

Command	Description
show diagnostic ondemand settings	Displays the settings for on-demand diagnostics.

diagnostic schedule module

To set the scheduling of test-based diagnostic testing for a specific module or schedule a supervisor engine switchover, use the **diagnostic schedule module** command in global configuration mode. To remove the scheduling, use the **no** form of this command.

diagnostic schedule module {*module-number* | *slot/subslot*} **test** {*test-id* | **all** | **complete** | **minimal** | **non-disruptive** | **per-port** [**port** | *interface-port-number* | *port-number-list* | **all**]} {**on** *month dd yyyy hh*:*mm* | **daily** *hh*:*mm* | **weekly** *day-of-week hh*:*mm*}

no diagnostic schedule module {*module-number* | *slot/subslot*} **test** {*test-id* | **all** | **complete** | **minimal** | **non-disruptive** | **per-port** [**port** | *interface-port-number* | *port-number-list* | **all**]} {**on** *month dd yyyy hh*:*mm* | **daily** *hh*:*mm* | **weekly** *day-of-week hh*:*mm*}

Syntax Description

module-number	Specifies the module number.
slot/subslot	Specifies the slot number of the active supervisor engine.
test	Specifies the diagnostic test suite attribute.
test-id	Identification number for the test to be run; see the "Usage Guidelines" section for additional information.
all	Runs all diagnostic tests.
complete	Selects the complete bootup test suite.
minimal	Selects the minimal bootup test suite.
non-disruptive	Selects the nondisruptive test suite.
per-port	Selects the per-port test suite.
port	(Optional) Specifies the port to schedule testing.
interface-port-number	(Optional) Port number.
port-number-list	(Optional) Range of port numbers, separated by a hyphen.
all	(Optional) Specifies all ports.
on *month dd yyyy hh*:*mm*	Specifies the scheduling of a test-based diagnostic task; see the "Usage Guidelines" section for formatting guidelines.
daily *hh*:*mm*	Specifies the daily scheduling of a test-based diagnostic task; see the "Usage Guidelines" section for formatting guidelines.
weekly *day-of-week hh*:*mm*	Specifies the weekly scheduling of a test-based diagnostic task; see the "Usage Guidelines" section for formatting guidelines.

Command Default

Test-based diagnostic testing for a specific module is not scheduled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was modified to support scheduled switchover for supervisor engines.
12.2(17d)SXB	This command was modified to support the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The **complete**, **minimal**, **non-disruptive**, and **per-port** keywords were added.

Usage Guidelines

Use these guidelines when scheduling testing:

- *test-id*—Enter the **show diagnostic content** command to display the test ID list.
- *month*—Spell out the month such as january, february ... december (either uppercase or lowercase characters).
- *dd*—Enter the day as a two-digit number.
- *yyyy*—Enter the year as a four-digit number.
- *hh***:***mm*—Enter the time as a two-digit number (for a 24-hour clock) for hours:minutes; the colon (**:**) is required.
- *day-of-week*—Spell out the day of the week, such as monday, tuesday... sunday (either uppercase or lowercase characters).
- **per-port** is not supported when specifying a scheduled switchover.

You can use the **diagnostic schedule module** *slot/subslot* **test** *test-id* command to schedule a switchover from the active supervisor engine to the standby supervisor engine.

Enter the **show diagnostic content module** *slot/subslot* command to display the test ID list and look for the test ID in the ScheduleSwitchover field.

You can specify a periodic switchover (daily or weekly) or a single switchover occurrence at a specific time using these commands:

- **diagnostic schedule module** *slot/subslot* **test** *test-id* **on** *mm dd yyyy hh:mm*
- **diagnostic schedule module** *slot/subslot* **test** *test-id* **daily** *hh:mm*
- **diagnostic schedule module** *slot/subslot* **test** *test-id* **weekly** *day-of-week hh:mm*

Note To avoid system downtime in the event that the standby supervisor engine cannot switch over the system, Cisco recommends that you schedule a switchover from the standby supervisor engine to the active supervisor engine 10 minutes after the switchover occurs.

Examples

The following example shows how to schedule the diagnostic testing on a specific month, date and time for a specific module:

```
Router(config)# diagnostic schedule module 1 test 5 on may 27 2010 10:30
```

The following example shows how to schedule the diagnostic testing to occur daily at a certain time for a specific module:

```
Router(config)# diagnostic schedule module 1 test 5 daily 12:25
```

The following example shows how to schedule the diagnostic testing to occur weekly on a certain day for a specific module:

```
Router(config)# diagnostic schedule module 1 test 5 weekly friday 09:23
```

Related Commands

Command	Description
show diagnostic content	Displays test information including test ID, test attributes, and supported coverage test levels for each test and for all modules.
show diagnostic schedule	Displays the current scheduled diagnostic tasks.

diagnostic start

To run the specified diagnostic test, use the **diagnostic start** command in privileged EXEC mode.

diagnostic start module *num* **test** {*test-id* | *test-id-range* | **minimal** | **complete** | **basic** | **per-port** | **non-disruptive** | **all**} [**port** {*num* | *port#-range* | **all**}]

diagnostic start system test all

Cisco UBR10012 Universal Broadband Router

diagnostic start {**bay** *slot/bay* | **slot** *slot-no*} **test** {*test-id* | *test-id-range* | **all** | **complete** | **minimal** | **non-disruptive**}

diagnostic start {**subslot** *slot/sub-slot*} **test** {*test-id* | *test-id-range* | **all** | **complete** | **minimal** | **non-disruptive** | **per-port** [**port** {num | *port#-range* | **all**}]}

Syntax Description

module *num*	Specifies the module number.
test	Specifies a test to run.
test-id	Identification number for the test to run. See the Usage Guidelines section for additional information.
test-id-range	Range of identification numbers for tests to run. See the Usage Guidelines section for additional information.
minimal	Runs minimal bootup diagnostic tests.
complete	Runs complete bootup diagnostic tests.
basic	Runs basic on-demand diagnostic tests.
per-port	Runs per-port level tests.
non-disruptive	Runs the non disruptive health-monitoring tests.
all	Runs all diagnostic tests.
port *num*	(Optional) Specifies the interface port number.
port *port#-range*	(Optional) Specifies the interface port number range. See the Usage Guidelines section for additional information.
port all	(Optional) Specifies all ports.
system test all	Runs all disruptive and nondisruptive diagnostic tests at once. All test dependencies are handled automatically.
bay *slot/bay*	Indicates the card slot and bay number where the diagnostic test is executed. The **bay** keyword is used to refer a SPA on the router. The valid range for the slot number is from 1 to 8 and 0 to 3 for the bay number.
slot *slot-no*	Indicates the slot number of the full-height line card where the diagnostic test is executed. The **slot** keyword is used to refer a full-height line card on the router. The valid range for slot is from 1 to 8.
subslot *slot/sub-slot*	Indicates the slot and subslot number of half-height line card where the diagnostic test is executed. The **subslot** keyword is used to refer a half-height line card on the router. The valid range for the slot number is from 1 to 8 and 0 to 1 for the subslot number.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed to include the **complete** and **basic** keywords.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2.(33)SXH	This command was changed to include the **system test all** keywords.
12.2(33)SCC	The command was integrated in this release to support Generic Online Diagnostics (GOLD) functionality for Cisco UBR10012 Universal Broadband Router. The keywords **bay**, **slot**, and **subslot** were added for the Cisco UBR10012 Universal Broadband Router.

Usage Guidelines

Note Running all online diagnostic tests disrupts normal system operation. Reset the system after the **diagnostic start system test all** command has completed.
Do not insert, remove, or power down line cards or the supervisor while the system test is running.
Do not issue any diagnostic command other than the **diagnostic stop system test all** command while the system test is running.
Make sure no traffic is running in background.

Note Do not enter the **diagnostic start module** *x* **test all** command on systems that are configured with a DFC3A because this command causes the TCAM test to fail.

Enter the **show diagnostic content** command to display the test ID list.

Enter the *test-id-range* or *port#-range* as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).

Use **diagnostic stop** command to stop the testing process.

Cisco UBR10012 Router

The command syntax to refer a line card or SPAs is different on Cisco UBR10012 Router. The keyword is **slot x** for a full-height line card, **slot x/y** for a half-height card, and **bay x/y** for a SPA.

Note To start a diagnostic test on the Cisco UBR10012 Router execute the command **diagnostic stop** with the **bay**, **slot** or **subslot** keyword respectively.

The GOLD test cases used to poll for system errors in Cisco IOS Software Release 12.2(33)SCC are Low Latency Queueing (LLQ) drop, Cable Line Card (CLC) memory leak, and Guardian index leak tests.

Examples

The following example shows how to run the specified diagnostic test at the specified slot:

```
Router# diagnostic start module 1 test 5
Module 1:Running test(s) 5 may disrupt normal system operation
Do you want to run disruptive tests? [no] yes
00:48:14:Running OnDemand Diagnostics [Iteration #1] ...
00:48:14:%DIAG-SP-6-TEST_RUNNING:Module 1:Running TestNewLearn{ID=5} ...
00:48:14:%DIAG-SP-6-TEST_OK:Module 1:TestNewLearn{ID=5} has completed successfully
00:48:14:Running OnDemand Diagnostics [Iteration #2] ...
00:48:14:%DIAG-SP-6-TEST_RUNNING:Module 1:Running TestNewLearn{ID=5} ...
00:48:14:%DIAG-SP-6-TEST_OK:Module 1:TestNewLearn{ID=5} has completed successfully
Router#
```

This example shows how to start all online diagnostic tests:

```
Router# diagnostic start system test all
**************************************************************************
* WARNING: *
* 'diagnostic start system test all' will disrupt normal system *
* operation. The system requires RESET after the command *
* 'diagnostic start system test all' has completed prior to *
* normal use. *
* *
* IMPORTANT: *
* 1. DO NOT INSERT, OIR, or POWER DOWN Linecards or *
* Supervisor while system test is running. *
* *
* 2. DO NOT ISSUE ANY DIAGNOSTIC COMMAND except *
* "diagnostic stop system test all" while system test *
* is running. *
* *
* 3. PLEASE MAKE SURE no traffic is running in background. *
**************************************************************************
Do you want to continue? [no]:
```

Cisco UBR10012 Router

The following example shows how to run a diagnostic test with test id 2 on a SPA:

```
ubr-122s-1# diagnostic start bay 1/0 test 2
ubr-122s-1#
Aug  5 09:24:42.019: %DIAG-6-TEST_RUNNING: Bay 1/0: Running TestModenaLLQDrops{I
D=2} ...
Aug  5 09:24:42.019: %DIAG-6-TEST_OK: Bay 1/0: TestModenaLLQDrops{ID=2} has comp
leted successfully
```

Related Commands

Command	Description
diagnostic schedule	Sets the diagnostic test schedule for a particular bay, slot, or subslot.
show diagnostic description	Provides the description for the diagnostic tests.
diagnostic stop	Runs the specified diagnostic test.
show diagnostic content module	Displays the available diagnostic tests.

Command	Description
diagnostic bootup level	Configures the diagnostic bootup level.
diagnostic event-log size	Modifies the diagnostic event-log size dynamically.
diagnostic monitor	Configures the health-monitoring diagnostic testing.
diagnostic ondemand	Configures the on-demand diagnostics.
show diagnostic bootup	Displays the configured diagnostics level at bootup.
show diagnostic events	Displays the diagnostic event log.
show diagnostic ondemand settings	Displays the settings for the on-demand diagnostics.
show diagnostic result	Displays the diagnostic test results for a module.
show diagnostic schedule	Displays the current scheduled diagnostic tasks.
show diagnostic status	Displays the running diagnostics tests.

diagnostic stop

To stop the testing process, use the **diagnostic stop** command in privileged EXEC mode.

diagnostic stop module *num*

Cisco UBR10012 Universal Broadband Router

diagnostic stop {**bay** *slot/bay* | **slot** *slot-no* | **subslot** *slot/subslot*}

Syntax Description

module *num*	Module number.
bay *slot/bay*	Indicates the card slot and bay number of the SPA for which the diagnostic test has stopped. The **bay** keyword is used to refer a SPA on the router. The valid range for the slot number is from 1 to 8 and 0 to 3 for the bay number.
slot *slot-no*	Indicates the slot number of full height line card for which the diagnostic test has to be stopped. The **slot** keyword is used to refer a full-height line card on the router. Valid range for the slot is from 1 to 8.
subslot *slot/subslot*	Indicates the slot and subslot number of half-height line card for which the diagnostic test has to be stopped. The **subslot** keyword is used to refer a half-height line card on the router. The valid range for the slot number is from 1 to 8 and 0 to 1 for the subslot number.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCC	The command was integrated in this release to support Generic Online Diagnostics (GOLD) functionality for Cisco UBR10012 Universal Broadband Router. The keywords **bay**, **slot**, and **subslot** were added for the Cisco UBR10012 Universal Broadband Router.

Usage Guidelines

Use the **diagnostic start** command to start the testing process.

Cisco UBR10012 Router

The command syntax to refer a line card or SPAs is different on Cisco UBR10012 Router. The keyword is **slot x** for a full-height line card, **slot x/y** for a half-height card, and **bay x/y** for a SPA.

Note To stop a diagnostic test on the Cisco UBR10012 Router execute the command **diagnostic stop** with the **bay**, **slot** or **subslot** keyword respectively.

The GOLD test cases used to poll for system errors in Cisco IOS Software Release 12.2(33)SCC are Low Latency Queueing (LLQ) drop, Cable Line Card (CLC) memory leak, and line card index leak tests.

Examples

This example shows how to stop the diagnostic test process:

```
Router# diagnostic stop module 3
Router#
```

This example shows how to stop the diagnostic test process for subslot 5/0 on the Cisco UBR10012 Universal Broadband Router:

```
Router# diagnostic stop subslot 5/0
Router#
```

Related Commands

Command	Description
diagnostic schedule	Sets the diagnostic test schedule for a particular bay, slot, or subslot.
show diagnostic description	Provides the description for the diagnostic tests.
diagnostic start	Stops the specified diagnostic test.
show diagnostic content module	Displays the available diagnostic tests.
diagnostic bootup level	Configures the diagnostic bootup level.
diagnostic event-log size	Modifies the diagnostic event-log size dynamically.
diagnostic monitor	Configures the health-monitoring diagnostic testing.
diagnostic ondemand	Configures the on-demand diagnostics.
show diagnostic bootup	Displays the configured diagnostics level at bootup.
show diagnostic events	Displays the diagnostic event log.
show diagnostic ondemand settings	Displays the settings for the on-demand diagnostics.
show diagnostic result	Displays the diagnostic test results for a module.
show diagnostic schedule	Displays the current scheduled diagnostic tasks.
show diagnostic status	Displays the running diagnostics tests.

dir

To display a list of files on a file system, use the **dir** command in EXEC, privileged EXEC, or diagnostic mode.

dir [**/all**] [**/recursive**] [**all-filesystems**] [*filesystem***:**] [*file-url*]

Syntax Description

/all	(Optional) Lists deleted files, undeleted files, and files with errors.
/recursive	(Optional) Lists files recursively.
all-filesystems	(Optional) Lists all files in all file systems on the router.
*filesystem***:**	(Optional) File system or directory containing the files to list, followed by a colon.
file-url	(Optional) The name of the files to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

Defaults

When you omit the **/all** keyword, the Cisco IOS software displays only undeleted files.

Command Modes

User EXEC (>)
Privileged EXEC (#)
Diagnostic (diag)

Command History

Release	Modification
11.0	This command was introduced.
12.3	This command was modified. A timestamp that shows the offset from Coordinated Universal Time (UTC) was added to the **dir** command display.
12.3(14)T	This command was modified. The **usbflash**[**0**-**9**]**:** and **usbtoken**[**0**-**9**]**:** options were added as available file systems.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was modified. Support for this command was implemented on the Cisco 7200VXR NPE-G2 platform.
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers, and the following enhancements were introduced: • The command was made available in diagnostic mode. • The **/recursive** option was introduced. • The file systems available with the Cisco ASR 1000 Series Routers became available as *filesystem*: options.
15.0(1)M	This command was modified. The output modifier was added.

Usage Guidelines

Use the **show** (flash file system) command to display more details about the files in a particular file system.

You can use the Cisco IOS software output modifiers to filter the output of the **dir** command, to display only those lines you are interested in.

The output modifier feature is invoked by using the pipe symbol (|). To use this feature, enter the **dir** command as normal but add a space and the pipe symbol at the end of the command line. Then add one of the keywords shown in Table 28.

Table 28 Using Output Modifiers

Command	Purpose
append *regular expression*	Appends redirected output to URL (only to the URLs supporting the append operation).
begin *regular expression*	Displays the first line that matches the regular expression, and then all other lines that follow that line.
include *regular expression*	Displays all lines that match the regular expression.
exclude *regular expression*	Displays all lines except those that match the regular expression.
format *regular expression*	Formats the output using the specification file.
redirect *regular expression*	Redirects the output to the URL.
section *regular expression*	Filters a section of the output.
tee *regular expression*	Copies output to the URL.

Note The **append**, **redirect** and **tee** keywords do not support rcp in the display.

Examples

The following is sample output from the **dir** command:

```
Router# dir slot0:

Directory of slot0:/

1  -rw-     4720148   Dec 29 2003 17:49:36  -08:00 hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Jan 02 2004 18:42:53  -08:00 c7200-js-mz
  5  -rw-         639   Jan 03 2004 12:09:32  -08:00 rally
  7  -rw-         639   Jan 03 2004 12:37:13  -08:00 the_time

20578304 bytes total (3104544 bytes free)
```

The following is sample output from the **dir /all** command:

```
Router# dir /all slot0:

Directory of slot0:/

1  -rw-     4720148   Dec 15 2003 17:49:36  -08:00 hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Jan 02 2004 18:42:53  -08:00 c7200-js-mz
  3  -rw-     7982828   Jan 02 2004 18:48:14  -08:00 [rsp-jsv-mz]
  4  -rw-         639   Jan 03 2004 12:09:17  -08:00 the_time]
  5  -rw-         639   Jan 03 1994 12:09:32  -08:00 rally
```

```
  6  -rw-          639   Jan 03 1994 12:37:01  -08:00 [the_time]
  7  -rw-          639   Jan 03 1994 12:37:13  -08:00
```

Table 29 describes the significant fields shown in the displays.

Table 29 dir Field Descriptions

Field	Description
1	Index number of the file.
-rw-	Permissions. The file can be any or all of the following: • d—directory • r—readable • w—writable • x—executable
4720148	Size of the file, in bytes.
Dec 15 2003 17:49:36	Last modification date.
-08:00	Conversion to local time in hours from Coordinated Universal Time (UTC). In the example, -08:00 indicates that the given time is 8 hours behind UTC or Pacific Standard Time (PST).
hampton/nitro/c7200-j-mz	Filename. Deleted files are indicated by square brackets around the filename.

The following example shows how to use the output modifier feature with the **exclude** keyword and regular expression. Table 29 describes the significant fields shown in the output.

```
Routwe# dir | exclude asr

Directory of bootflash:/

   12  drwx        4096   Jan 5 2005 01:34:50 +00:00  lost+found
59265  drwx        4096  Apr 20 2004 01:51:10 +00:00  .installer
14817  drwx        4096  Apr 20 2004 01:54:37 +00:00  .ssh
88897  drwx        4096   Jan 7 2005 22:13:26 +00:00  .prst_sync
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
delete	Deletes a file on a Flash memory device.
undelete	Recovers a file marked “deleted” on a Class A or Class B flash file system.

disable

To exit privileged EXEC mode and return to user EXEC mode, or to exit to a lower privilege level, enter the **disable** command in EXEC, privileged EXEC, or diagnostic mode.

disable [*privilege-level*]

Syntax Description

privilege-level	(Optional) Specific privilege level (other than user EXEC mode).

Command Modes

EXEC (>)
Privileged EXEC (#)
Diagnostic (diag)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers, and became available in diagnostic mode.

Usage Guidelines

Up to 16 security levels can be configured using Cisco IOS software. If such levels are configured on a system, using this command with the *privilege-level* option allows you to exit to a lower security level. If a level is not specified, the user will exit to the user EXEC mode, which is the default.

Note Five EXEC commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure a privilege level greater than 0, these five commands will not be included in the command set for that privilege level.

Examples

In the following example, the user enters privileged EXEC mode using the **enable** command, then exits back to user EXEC mode using the **disable** command. Note that the prompt for user EXEC mode is >, and the prompt for privileged EXEC mode is #.

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

Related Commands

Command	Description
enable	Enables higher privilege level access, such as privileged EXEC mode.

disconnect-character

To define a character to disconnect a session, use the **disconnect-character** command in line configuration mode. To remove the disconnect character, use the **no** form of this command.

disconnect-character *ascii-number*

no disconnect-character

Syntax Description

ascii-number	Decimal representation of the session disconnect character.

Defaults

No disconnect character is defined.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

See the "ASCII Character Set and Hex Values" appendix for a list of ASCII characters.

The Break character is represented by zero; NULL cannot be represented.

To use the session-disconnect character in normal communications, precede it with the escape character.

Examples

The following example defines the disconnect character for virtual terminal line 4 as Escape, which is decimal character 27:

```
Router(config)# line vty 4
Router(config-line)# disconnect-character 27
```

dispatch-character

To define a character that causes a packet to be sent, use the **dispatch-character** command in line configuration mode. To remove the definition of the specified dispatch character, use the **no** form of this command.

dispatch-character *ascii-number1* [*ascii-number2 . . . ascii-number*]

no dispatch-character *ascii-number1* [*ascii-number2 . . . ascii-number*]

Syntax Description

ascii-number1	Decimal representation of the desired dispatch character.
ascii-number2 . . . ascii-number	(Optional) Additional decimal representations of characters. This syntax indicates that you can define any number of characters as dispatch characters.

Defaults

No dispatch character is defined.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

See the "ASCII Character Set and Hex Values" appendix for a list of ASCII characters.

The **dispatch-character** command defines one or more dispatch characters that cause a packet to be sent even if the dispatch timer has not expired. Use of a dispatch character causes the Cisco IOS software to attempt to buffer characters into larger-sized packets for transmission to the remote host.

Enable the **dispatch-character** command from the session that initiates the connection, not from the incoming side of a streaming Telnet session.

This command can take multiple arguments, so you can define any number of characters as dispatch characters.

Examples

The following example defines the Return character (decimal 13) as the dispatch character for virtual terminal line (vty) line 4:

```
Router(config)# line vty 4
Router(config-line)# dispatch-character 13
```

Related Commands

Command	Description
dispatch-machine	Specifies an identifier for a TCP packet dispatch state machine on a particular line.
dispatch-timeout	Sets the character dispatch timer.
state-machine	Specifies the transition criteria for the state of a particular state machine.
terminal dispatch-character	Defines a character that causes a packet to be sent for the current session.

dispatch-machine

To specify an identifier for a TCP packet dispatch state machine on a particular line, use the **dispatch-machine** command in line configuration mode. To disable a state machine on a particular line, use the **no** form of this command.

dispatch-machine *name*

no dispatch-machine

Syntax Description

name	Name of the state machine that determines when to send packets on the asynchronous line.

Defaults

No dispatch state machine identifier is defined.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When the **dispatch-timeout** command is specified, a packet being built will be sent when the timer expires, and the state will be reset to zero.

Any dispatch characters specified using the **dispatch-character** command are ignored when a state machine is also specified.

If a packet becomes full, it will be sent regardless of the current state, but the state will not be reset. The packet size depends on the traffic level on the asynchronous line and the dispatch-timeout value. There is always room for 60 data bytes. If the dispatch-timeout value is greater than or equal to 100 milliseconds, a packet size of 536 (data bytes) is allocated.

Examples

The following example specifies the name linefeed for the state machine:

```
Router(config)# state-machine linefeed 0 0 9 0
Router(config)# state-machine linefeed 0 11 255 0
Router(config)# state-machine linefeed 0 10 10 transmit
Router(config)# line 1
Router(config-line)# dispatch-machine linefeed
```

Related Commands

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

Command	Description
dispatch-timeout	Sets the character dispatch timer.
state-machine	Specifies the transition criteria for the state of a particular state machine.

dispatch-timeout

To set the character dispatch timer, use the **dispatch-timeout** command in line configuration mode. To remove the timeout definition, use the **no** form of this command.

dispatch-timeout *milliseconds*

no dispatch-timeout

Syntax Description

milliseconds	Integer that specifies the number of milliseconds (ms) that the Cisco IOS software waits after putting 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.

Defaults

No dispatch timeout is defined.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to increase the processing efficiency for 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 **dispatch-timeout** and **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 system response time might appear intermittent if the timeout interval is greater than 100 milliseconds and remote echoing is used. For lines with a reverse-Telnet connection, use a dispatch-timeout value less than 10 milliseconds.

Examples

The following example sets the dispatch timer to 80 milliseconds for virtual terminal line (vty) lines 0 through 4:

```
Router(config)# line vty 0 4
Router(config-line)# dispatch-timeout 80
```

Related Commands

Command	Description
buffer-length	Specifies the maximum length of data streams forwarded on a line.
dispatch-character	Defines a character that causes a packet to be sent.
dispatch-machine	Specifies an identifier for a TCP packet dispatch state machine on a particular line.
state-machine	Specifies the transition criteria for the state of a particular state machine.
terminal dispatch-timeout	Sets the character dispatch timer for the current session.

do

To execute user EXEC or privileged EXEC commands from global configuration mode or other configuration modes or submodes, use the **do** command in any configuration mode.

do *command*

Syntax Description

command	The user EXEC or privileged EXEC command to be executed.

Command Default

A user EXEC or privileged EXEC command is not executed from a configuration mode.

Command Modes

All configuration modes

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(17a)SX	This command was changed to support the **copy** command restriction.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to execute user EXEC or privileged EXEC commands (such as **show**, **clear**, and **debug** commands) while configuring your routing device. After the EXEC command is executed, the system will return to the configuration mode you were using.

Tip This command can be useful for saving your configuration to the startup-config file without having to return to the user EXEC mode or privileged EXEC mode (**do copy running-config startup-config**) or for checking the status of a feature (using a **do show** command) while configuring the feature.

Caution Do not enter the **do** command in user EXEC mode or privileged EXEC mode. Interruption of service might occur.

You cannot use the **do** command to execute the **configure terminal** command because entering the **configure terminal** command changes the user EXEC mode or privileged EXEC mode to the global configuration mode.

You cannot use the **do** command to execute **copy** or **write** commands in the global configuration or any other configuration mode or submode.

Examples

The following example shows how to enter the **show interfaces serial** privileged EXEC command from within global configuration mode:

```
Router(config)# do show interfaces serial 3/0

Serial3/0 is up, line protocol is up
  Hardware is M8T-RS232
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output 1d17h, output hang never
  Last clearing of "show interface" counters never
.
.
.
```

The following example shows how to enter the **clear vpdn tunnel** user EXEC or privileged EXEC command from within VPDN configuration mode:

```
Router(config-vpdn)# do clear vpdn tunnel
```

Related Commands

Command	Description
clear vpdn tunnel	Shuts down a specified VPDN tunnel and all sessions within the tunnel.
configure terminal	Enters global configuration mode.
copy	Copies any file from a source to a destination.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
write core	Tests the configuration of a core dump setup.

downward-compatible-config

To generate a configuration that is compatible with an earlier Cisco IOS release, use the **downward-compatible-config** command in global configuration mode. To disable this function, use the **no** form of this command.

downward-compatible-config *version*

no downward-compatible-config

Syntax Description

version	Cisco IOS release number, not earlier than Release 10.2. **Note** You must have a period (**.**) in the version number. For example, 12.4.

Defaults

The configuration is not compatible with earlier Cisco IOS releases.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

In Cisco IOS Release 10.3, IP access lists changed format. Use the **downward-compatible-config** command to regenerate a configuration in a format prior to Release 10.3 if you will downgrade from your software version to version 10.2 or 10.3. The earliest *version* value this command accepts is 10.2.

When this command is configured, the router attempts to generate a configuration that is compatible with the specified version. Note that this command affects only IP access lists.

Under some circumstances, the software might not be able to generate a fully backward-compatible configuration. In such a case, the software issues a warning message.

Examples

The following example shows how to generate a configuration file compatible with Cisco IOS Release 10.2 access lists:

```
Router(config)# downward-compatible-config 10.2
```

Related Commands

Command	Description
access-list (extended)	Provides extended access lists that allow more detailed access lists.
access-list (standard)	Defines a standard XNS access list.

editing

To reenable Cisco IOS enhanced editing features for a particular line after they have been disabled, use the **editing** command in line configuration mode. To disable these features, use the **no** form of this command.

editing

no editing

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Enhanced editing features are enabled by default. However, there may be situations in which you need to disable these features. The **no** form of this command disables these enhanced editing features, and the plain form of the command can be used to reenable these features.

Table 30 provides a description of the keys used to enter and edit commands when the editing features are enabled. Ctrl indicates the Control key, which must be pressed simultaneously with its associated letter key. Esc indicates the Escape key, which must be pressed first, followed by its associated letter key. A comma is used in the following table to indicate a key sequence (the comma key should not be pressed). Keys are not case sensitive. Many letters used for CLI navigation and editing were chosen to provide an easy way of remembering their functions. In the following table (Table 30), characters are bolded in the “Function Summary” column to indicate the relation between the letter used and the function.

Table 30 Command Editing Keys and Functions

Keys	Function Summary	Function Details
Tab	Complete command	Completes a partial command name entry. When you enter a unique set of characters and press the Tab key, the system completes the command name. If you enter a set of characters that could indicate more than one command, the system beeps to indicate an error. To view the commands which match the set of characters you have entered, enter a question mark (?) immediately following the partial command (no space). The CLI will then list the commands that begin with that string.
Return (at the command line)	Execute	Executes the command.
Return (at the --More--prompt)	Continue	Displays the next line of output.
Space Bar (at the --More--prompt)	Continue	Displays the next screen of output. The amount of output you see will depend on the screen depth setting of your terminal.
Delete or Backspace	Backspace	Erases the character to the left of the cursor.
Left Arrow[1] or Ctrl-B	**B**ack character	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry.
Right Arrow[1] or Ctrl-F	**F**orward character	Moves the cursor one character to the right.
Esc, B	**B**ack word	Moves the cursor back one word.
Esc, F	**F**orward word	Moves the cursor forward one word.
Ctrl-A	Beginning of line	Moves the cursor to the beginning of the line.
Ctrl-E	**E**nd of line	Moves the cursor to the end of the command line.
Ctrl-D	**D**elete character	Deletes the character at the cursor.
Esc, D	**D**elete next word	Deletes from the cursor to the end of the word.
Ctrl-W	Delete previous **w**ord	Deletes the word to the left of the cursor.
Ctrl-K	Delete line forward	Deletes all characters from the cursor to the end of the command line.
Ctrl-U or Ctrl-X	Delete line backward	Deletes all characters from the cursor back to the beginning of the command line.
Ctrl-T	**T**ranspose characters	Transposes the character to the left of the cursor with the character located at the cursor.

Table 30 Command Editing Keys and Functions (continued)

Keys	Function Summary	Function Details
Ctrl-R or Ctrl-L	**R**edisplay **l**ine	Redisplays the system prompt and command line.
Ctrl-V or Esc, Q	Ignore editing	Inserts a code to indicate to the system that the keystroke immediately following should be treated as a command entry, *not* as an editing key.
Up Arrow[1] or Ctrl-P	**P**revious command	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down Arrow[1] or Ctrl-N (next)	**N**ext command	Returns to more recent commands in the history buffer (after recalling commands with the Up Arrow or Ctrl-P). Repeat the key sequence to recall successively more recent commands.
Ctrl-Y	Recall last deleted command	Recalls the most recent entry in the delete buffer. The delete buffer contains the last ten items you have deleted or cut. Ctrl-Y can be used in conjunction with Esc Y.
Esc, Y	Recall next deleted command	Recalls the next entry in the delete buffer. The delete buffer contains the last ten items you have deleted. Press Ctrl-Y first to recall the most recent entry. Then press Esc Y up to nine times to recall the remaining entries in the buffer. If you bypass an entry, continue to press Esc Y to cycle back to it.
Esc, C	**C**apitalize word	Capitalizes the word from the cursor to the end of the word.
Esc, U	Make word **u**ppercase	Changes all letters from the cursor to the next space on the line appear in uppercase letters.
Esc, L	Make word **l**owercase	Changes the word to lowercase from the cursor to the end of the word.

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

Examples

In the following example, enhanced editing mode is disabled on line 3:

```
Router(config)# line 3
Router(config-line)# no editing
```

Related Commands

Command	Description
terminal editing	Controls CLI enhanced editing feature for the current terminal session.

enable

To change the privilege level for a CLI session or to use a CLI view for a CLI session, use the **enable** command in either user EXEC, privileged EXEC, or diagnostic mode.

enable [*privilege-level*] [**view** [*view-name*]]

Syntax Description

privilege-level	(Optional) Privilege level at which to log in.
view	(Optional) Enters into root view, which enables users to configure CLI views. **Note** This keyword is required if you want to configure a CLI view.
view-name	(Optional) Enters or exits a specified command-line interface (CLI) view. This keyword can be used to switch from one CLI view to another CLI view.

Defaults

Privilege-level 15 (privileged EXEC)

Command Modes

User EXEC (>)

Privileged EXEC (#)

Diagnostic Mode (diag)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	The **view** keyword and *view-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **view** keyword and *view-name* argument were integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(22)SB.
Cisco IOS XE Release 2.1	This command became available on the ASR 1000 Series Routers, and became available in diagnostic mode for the first time.

Usage Guidelines

By default, using the **enable** command without the *privilege-level* argument in user EXEC mode causes the router to enter privileged EXEC mode (privilege-level 15).

Entering privileged EXEC mode enables the use of privileged commands. Because many of the privileged commands set operating parameters, privileged access should be password-protected to prevent unauthorized use. If the system administrator has set a password with the **enable password** global configuration command, you are prompted to enter the password before being allowed access to privileged EXEC mode. The password is case sensitive.

If an **enable** password has not been set, only enable mode can be accessed through the console connection.

Security levels can be set by an administrator using the **enable password** and **privilege level** commands. Up to 16 privilege levels can be specified, using the numbers 0 through 15. Using these privilege levels, the administrator can allow or deny access to specific commands. Privilege level 0 is associated with user EXEC mode, and privilege level 15 is associated with privileged EXEC mode.

For more information on defined privilege levels, see the *Cisco IOS Security Configuration Guide* and the *Cisco IOS Security Command Reference* publications.

If a level is not specified when entering the **enable** command, the user will enter the default mode of privileged EXEC (level 15).

Accessing a CLI View

CLI views restrict user access to specified CLI and configuration information. To configure and access CLI views, users must first enter into root view, which is accomplished via the **enable view** command (without the *view-name* argument). Thereafter, users are prompted for a password, which is the same password as the privilege level 15 password.

The *view-name* argument is used to switch from one view to another view.

To prevent dictionary attacks, a user is prompted for a password even if an incorrect view name is given. The user is denied access only after an incorrect view name and password are given.

Examples

In the following example, the user enters privileged EXEC mode (changes to privilege-level 15) by using the **enable** command without a privilege-level argument. The system prompts the user for a password before allowing access to the privileged EXEC mode. The password is not printed to the screen. The user then exits back to user EXEC mode using the **disable** command. Note that the prompt for user EXEC mode is the greater than symbol (>), and the prompt for privileged EXEC mode is the number sign (#).

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

The following example shows which commands are available inside the CLI view “first” after the user has logged into this view:

```
Router# enable view first

Password:

00:28:23:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
Router# ?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information

Router# show ?

  ip       IP information
  parser   Display parser information
  version  System hardware and software status
```

```
Router# show ip ?

  access-lists            List IP access lists
  accounting              The active IP accounting database
  aliases                 IP alias table
  arp                     IP ARP table
  as-path-access-list     List AS path access lists
  bgp                     BGP information
  cache                   IP fast-switching route cache
  casa                    display casa information
  cef                     Cisco Express Forwarding
  community-list          List community-list
  dfp                     DFP information
  dhcp                    Show items in the DHCP database
  drp                     Director response protocol
  dvmrp                   DVMRP information
  eigrp                   IP-EIGRP show commands
  extcommunity-list       List extended-community list
  flow                    NetFlow switching
  helper-address          helper-address table
  http                    HTTP information
  igmp                    IGMP information
  irdp                    ICMP Router Discovery Protocol
.
.
```

The following example shows how to use the **enable view** command to switch from the root view to the CLI view “first”:

```
Router# enable view
Router#
01:08:16:%PARSER-6-VIEW_SWITCH:successfully set to view 'root'.
Router#
! Enable the show parser view command from the root view
Router# show parser view

Current view is 'root'
! Enable the show parser view command from the root view to display all views
Router# show parser view all

Views Present in System:
View Name:   first
View Name:   second
! Switch to the CLI view “first.”
Router# enable view first
Router#
01:08:09:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
! Enable the show parser view command from the CLI view “first.”
Router# show parser view

Current view is 'first'
```

Related Commands

Command	Description
disable	Exits from privileged EXEC mode to user EXEC mode, or, if privilege levels are set, to the specified privilege level.
enable password	Sets a local password to control access to various privilege levels.
privilege level (global)	Sets a privilege level for a command.
privilege level (line)	Sets a privilege level for a command for a specific line.

enable last-resort

To enable password parameters as the last resort without specifying the local enable password if no TACACS servers respond, use the **enable last-resort** command in global configuration mode. To disable the password parameters, use the **no** form of this command.

enable last-resort {**password** | **succeed**}

no enable last-resort

Syntax Description

password	Enables password parameters by specifying the local enable password.
succeed	Enables password parameters without specifying the local enable password.

Command Default

The password parameters for the router are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS 15.0(1)M.

Examples

The following example shows how to enable password parameters as the last resort without specifying the local enable password if no TACACS servers respond:

```
Router> enable
Router# configure terminal
Router(config)# enable last-resort succeed
```

Related Commands

Command	Description
show tacacs	Displays statistics for a TACACS+ server.

end

To end the current configuration session and return to privileged EXEC mode, use the **end** command in global configuration mode.

end

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command will bring you back to privileged EXEC mode regardless of what configuration mode or configuration submode you are in.

Note This global configuration command can be used in any configuration mode.

Use this command when you are done configuring the system and you want to return to EXEC mode to perform verification steps.

Examples

In the following example, the **end** command is used to exit from ALPS ASCU configuration mode and return to privileged EXEC mode. A **show** command is used in privileged EXEC mode to verify the configuration.

```
Router# configure terminal
Router(config)# interface serial 1:1
Router(config-if)# alps ascu 4B
Router(config-alps-ascu)# end
Router# show interface serial 1:1
```

Related Commands

Command	Description
exit (global)	Exits from the current configuration mode.

environment-monitor shutdown temperature

To enable monitoring of the environment sensors, use the **environment-monitor shutdown temperature** command in global configuration mode. To disable monitoring of the environment sensors, use the **no** form of this command.

environment-monitor shutdown temperature [**rommon** | **powerdown**]

no environment-monitor shutdown temperature [**rommon** | **powerdown**]

Syntax Description

rommon	(Optional) Places the supervisor engine in ROMMON when a major active alarm is identified.
powerdown	(Optional) Powers down the supervisor engine when a new active major alarm is identified.

Defaults

By default, **rommon** is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXF17	Support for **powerdown** keyword added.
12.2(33)SXH6	Support for **powerdown** keyword added.

Examples

This example shows how to place the supervisor engine in ROMMON when a major active alarm occurs:

```
Router(config)# environment-monitor shutdown temperature rommon
Router(config)#
```

This example shows how to power down the supervisor engine when a major active alarm occurs:

```
Router(config)# environment-monitor shutdown temperature powerdown
Router(config)#
```

environment temperature-controlled

To enable the ambient temperature control, use the **environment temperature-controlled** command in global configuration mode. To disable the ambient temperature control, use the **no** form of this command.

environment temperature-controlled

no environment temperature-controlled

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command does not affect temperature monitoring and alarm thresholds; it only affects whether a module may be powered on. The software does not validate the inlet temperature.

If you enter the **no** form of this command and the cooling capacity is reduced below the module cooling requirement, a syslog warning (and SNMP alarm) is generated. This module status does not change, and an environmental alarm is not raised when you enter the **no** form of this command.

Examples

This example shows how to enable the ambient temperature control:

```
Router(config)# environment temperature-controlled
Router(config)#
```

This example shows how to disable the ambient temperature control:

```
Router(config)# no environment temperature-controlled
Router(config)#
```

erase

To erase a file system or all files available on a file system, use the **erase** command in privileged EXEC or diagnostic mode.

erase {**/all nvram:** | **/no-squeeze-reserve-space** *file-system***:** | *file-system***:** | **startup-config**}

Cisco 7600 Series Routers and Cisco ASR 1000 Series Routers

erase {**/all nvram:** | *file-system***:** | **startup-config**}

Syntax Description

/all	Erases all files in the specified file system.
nvram:	Erases all files in the NVRAM.
*file-system***:**	File system name, followed by a colon. For example, **flash:** or **nvram:**. **Note** This argument may not be used if the device memory contains logging persistent files.
/no-squeeze-reserve-space	Disables the squeeze operation to conserve memory and makes the **erase** command compatible with older file systems.
startup-config	Erases the contents of the configuration memory.

Command Modes

Privileged EXEC (#)
Diagnostic (#)

Command History

Release	Modification
11.0	This command was introduced.
12.2(11)T	This command was modified. The **/no-squeeze-reserve-space** keyword was added.
12.2(14)SX	This command was modified. Support for this command was added for the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was modified. The command was introduced in diagnostic mode on the Cisco ASR 1000 Series Routers, and the **/all** keyword was added.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The *file-system***:** argument was added.

Usage Guidelines

The **erase nvram:** command replaces the **write erase** command and the **erase startup-config** command.

Caution When you use the **erase** command to erase a file system, you cannot recover the files in the file system.

The *word help* feature is disabled for the **erase** command. You must enter the complete command name to enable the command. The parser does not complete the command name if you enter partial syntax of the command and press the Tab key. For more information on the *word help* feature, refer to the *Using the Cisco IOS Command-Line Interface* feature guide.

The **erase** command can be used on Class B and Class C flash file systems only.

Class A flash file systems cannot be erased. You can delete individual files using the **delete** command and then reclaim the space using the **squeeze** command. You can use the **format** command to format the flash file system. The **format** command when used on ATA disk clears the File Allocation Table (FAT) and root directory entries only. The data is not erased.

The **erase nvram:** command erases NVRAM. On Class A file system platforms, if the CONFIG_FILE variable specifies a file in flash memory, the specified file will be marked "deleted."

The **erase /all nvram:** command erases all files on NVRAM, including private NVRAM.

The **/no-squeeze-reserve-space** keyword is available on systems with small amounts of flash memory in order to conserve memory. When a squeeze operation is performed, the last two erase sectors are permanently reserved for the squeeze logs and squeeze buffer. The **/no-squeeze-reserve-space** keyword prevents the reservation of space that guarantees the ability to run the squeeze command. Disabling the squeeze operation keeps these memory sectors free. If any sectors using squeeze data are detected, they will be erased when the **/no-squeeze-reserve-space** keyword is used. The **/no-squeeze-reserve-space** keyword increases the available amount of usable flash space, but you may not be able to run the **squeeze** command. This is typically fine if the file system (such as flash) is used to store a single, large file. For example, an IOS image.

On Class C flash file systems, space is dynamically reclaimed when you use the **delete** command. You can also use either the **format** or **erase** command to reinitialize a Class C flash file system.

Note Use the context-sensitive help to determine which file systems can be used for the **erase** command. The output will vary based on the platform.

Examples

The following example shows how to erase the NVRAM, including the startup configuration located there:

```
Router# erase nvram:
```

The following example shows how to erase all of partition 2 in internal flash memory:

```
Router# erase flash:2

System flash directory, partition 2:
File  Length   Name/status
  1   1711088  dirt/images/c3600-i-mz
[1711152 bytes used, 15066064 available, 16777216 total]
Erase flash device, partition 2? [confirm]
Are you sure? [yes/no]: yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
```

The following example shows how to erase flash memory when flash is partitioned, but no partition is specified in the command:

```
Router# erase flash:

System flash partition information:
Partition    Size      Used     Free     Bank-Size    State        Copy-Mode
    1        4096K     2048K    2048K    2048K        Read Only    RXBOOT-FLH
```

```
    2       4096K    2048K   2048K   2048K       Read/Write  Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 2]
```

The system will prompt only if there are two or more read/write partitions. If the partition entered is not valid or is the read-only partition, the process terminates. You can enter a partition number, a question mark (**?**) for a directory display of all partitions, or a question mark and a number (**?***number*) for directory display of a particular partition. The default is the first read/write partition.

```
System flash directory, partition 2:
File  Length   Name/status
  1   3459720  master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]
Erase flash device, partition 2? [confirm] <Return>
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
delete	Deletes a file on a flash memory device.
more nvram:startup-config	Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
squeeze	Removes all deleted files from the flash file system and recovers the memory space used by deleted files.
undelete	Recovers a file marked “deleted” on a Class A or Class B flash file system.
write erase	The **write erase** command is replaced by the **erase nvram:** command. See the description of the **erase** command for more information

erase bootflash

The **erase bootflash:** and **erase bootflash** commands have identical functions. See the description of the **erase** command in this chapter for more information.

errdisable detect cause

To enable error-disable detection, use the **errdisable detect cause** command in global configuration mode. To disable error-disable detection, use the **no** form of this command.

errdisable detect cause {**all** | **bpduguard** | **dtp-flap** | **l2ptguard** | **link-flap** | **packet-buffer-error** | **pagp-flap** | **rootguard** | **udld**}

no errdisable detect cause {**all** | **bpduguard** | **dtp-flap** | **l2ptguard** | **link-flap** | **pagp-flap** | **rootguard** | **udld**}

Syntax Description

all	Specifies error-disable detection for all error-disable causes.
bpduguard	Specifies detection for the Bridge Protocol Data Unit (BPDU)-guard error-disable cause.
dtp-flap	Specifies detection for the Dynamic Trunking Protocol (DTP)-flap error-disable cause.
l2ptguard	Specifies detection for the Layer 2 Protocol Tunneling guard error-disable cause.
link-flap	Specifies detection for the link flap error-disable cause.
packet-buffer-error	Causes the packet buffer error to error-disable the affected port.
pagp-flap	Specifies detection for the Port Aggregation Protocol (PAgP)-flap error-disable cause.
rootguard	Specifies detection for the root-guard error-disable cause.
udld	Specifies detection for the Unidirectional Link Detection (UDLD) error-disable cause.

Defaults

Error-disable detection is enabled for all causes.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(14)SX	This command was modified. Support was added for the Supervisor Engine 720.
12.2(17b)SXA	This command was modified. The **packet-buffer-error** keyword was added.
12.2(17d)SXB	This command was modified. Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Note Entering the **no errdisable detect cause packet-buffer-error** command allows you to detect the fault that triggers a power cycle of the affected module.

A cause (bpduguard, dtp-flap, link-flap, pagp-flap, root-guard, udld) is defined as the reason why the error-disable state occurred. When a cause is detected on an interface, the interface is placed in an error-disable state (an operational state that is similiar to the link-down state).

You must enter the **shutdown** and then the **no shutdown** commands to recover an interface manually from the error-disable state.

Examples

The following example shows how to enable error-disable detection for the Layer 2 protocol-tunnel guard error-disable cause:

```
Router(config)# errdisable detect cause l2ptguard
```

Related Commands

Command	Description
show errdisable detect	Displays the error-disable detection status.
show interfaces status	Displays the interface status or a list of interfaces in an error-disable state on LAN ports only.
shutdown	Disables an interface.

errdisable recovery

To configure recovery mechanism variables, use the **errdisable recovery** command in global configuration mode. To return to the default state, use the **no** form of this command.

errdisable recovery {**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **psecure-violation** | **security-violation** | **rootguard** | **udld** | **unicast-flood**} | **interval** *seconds*}

no errdisable recovery {**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **psecure-violation** | **security-violation** | **rootguard** | **udld** | **unicast-flood**} | **interval** *seconds*}

Syntax Description

cause	Enables error-disable recovery from a specific cause.
all	Enables the recovery timers for all error-disable causes.
arp-inspection	Enables error-disable recovery from an Address Resolution Protocol (ARP) inspection cause.
bpduguard	Enables the recovery timer for the Bridge Protocol Data Unit (BPDU)-guard error-disable cause.
channel-misconfig	Enables the recovery timer for the channel-misconfig error-disable cause.
dhcp-rate-limit	Enables the recovery timer for the Dynamic Host Configuration Protocol (DHCP)-rate-limit error-disable cause.
dtp-flap	Enables the recovery timer for the Dynamic Trunking Protocol (DTP)-flap error-disable cause.
gbic-invalid	Enables the recovery timer for the Gigabit Interface Converter (GBIC)-invalid error-disable cause.
l2ptguard	Enables the recovery timer for the Layer 2 Protocol Tunneling (L2PT) error-disable cause.
link-flap	Enables the recovery timer for the link-flap error-disable cause.
pagp-flap	Enables the recovery timer for the Port Aggregation Protocol (PAgP)-flap error-disable cause.
psecure-violation	Enables the recovery timer for the psecure-violation error-disable cause.
security-violation	Enables the automatic recovery of ports that were disabled because of 802.1X security violations.
rootguard	Enables the recovery timer for the root-guard error-disable cause.
udld	Enables the recovery timer for the Unidirectional Link Detection (UDLD) error-disable cause.
unicast-flood	Enables the recovery timer for the unicast-flood error-disable cause.
interval *seconds*	Specifies the time, in seconds, to recover from a specified error-disable cause. The range is from 30 to 86400. The default interval is 300.

Command Default

The recovery mechanisms are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(14)SX	This command was modified. This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. This command was implemented on the Supervisor Engine 2.
12.2(18)SXD	This command was modified. The **arp-inspection** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

A cause (bpduguard, channel-misconfig, dhcp-rate-limit, dtp-flap, l2ptguard, link-flap, pagp-flap, psecure-violation, security-violation, rootguard, udld, or unicast-flood) is defined as the reason why the error-disable state occurred. When a cause is detected on an interface, the interface is placed in an error-disable state (an operational state that is similar to the link-down state). If you do not enable error-disable recovery for the cause, the interface stays in the error-disable state until a shutdown and no shutdown occur. If you enable recovery for a cause, the interface is brought out of the error-disable state and allowed to retry operation once all the causes have timed out.

You must enter the **shutdown** command and then the **no shutdown** command to manually recover an interface from the error-disable state.

Note A separate line is required each time you want to enter the **errdisable recovery cause** command to add a new reason for recovery; each new reason does not get appended to the original single line. This means you must enter each new reason separately.

Examples

This example shows how to enable the recovery timer for the BPDU-guard error-disable cause:

```
Router(config)# errdisable recovery cause bpduguard
```

This example shows how to set the recovery timer to 300 seconds:

```
Router(config)# errdisable recovery interval 300
```

Related Commands

Command	Description
show errdisable recovery	Displays the information about the error-disable recovery timer.
show interfaces status	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
shutdown	Disables an interface.

escape-character

To define a system escape character, use the **escape-character** command in line configuration mode. To set the escape character to Break, use the **no** or **default** form of this command.

escape-character {**break** | *char* | **default** | **none** | **soft**}

no escape-character [**soft**]

default escape-character [**soft**]

Syntax Description

break	Sets the escape character to Break. Note that the Break key should not be used as an escape character on a console terminal.
char	Character (for example, **!**) or its ASCII decimal representation (integer in the range of 0 to 255) to be used as the escape character.
default	Sets the escape key sequence to the default of Ctrl-^, X.
none	Disables escape entirely.
soft	Sets an escape character that will wait until pending input is processed before it executes.

Defaults

The default escape key sequence is Ctrl-Shift-6 (Ctrl-^) or Ctrl-Shift-6, X (^^X). The X is generally only required for modem connections.

The **default escape-character** command sets the escape character to Break (the default setting for Break is Ctrl-C).

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	The **soft** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

See the "ASCII Character Set and Hexidecimal Values" appendix for a list of ASCII characters.

The escape character (or key sequence) suspends any actively running processes and returns you to privileged EXEC mode or, if a menu is being used, to the system menu interface. The escape character is used for interrupting or aborting a process started by previously executed command. Examples of processes from which you can escape include Domain-Name lookup, **ping**, **trace**, and Telnet sessions initiated from the device to which you are connected.

To view the current setting of the escape sequence for a line, use the **show line** command followed by the specific line identifier (for example, **show line 0**, or **show line console**). The default escape sequence for a line is often displayed as ^^X . The first caret symbol represents the Control (Ctrl) key, the second caret symbol is literal (Shift-6), and the X is literal (for most systems, the X is not required).

To set the escape key for the active terminal line session, use the **terminal escape-character** command.

The Break key cannot be used as an escape character on a console terminal because the Cisco IOS software interprets Break as an instruction to halt the system. Depending upon the configuration register setting, break commands issued from the console line either will be ignored or cause the server to shut down.

To send an escape sequence over a Telnet connection, press **Ctrl-Shift-6** twice.

The **escape-character soft** form of this command defines a character or character sequence that will cause the system to wait until pending input is processed before suspending the current session. This option allows you to program a key sequence to perform multiple actions, such as using the F1 key to execute a command, then execute the escape function after the first command is executed.

The following restrictions apply when using the **soft** keyword:

- The length of the logout sequence must be 14 characters or fewer.
- The soft escape character cannot be the same as the generic Cisco escape character, Break, or the characters b, d, n, or s.
- The soft escape character should be an ASCII value from 1 to 127. Do not use the number 30.

Examples

The following example sets the escape character for the console line to the keyboard entry Ctrl-P, which is represented by the ASCII decimal value of 16:

```
Router(config)# line console
Router(config-line)# escape-character 16
```

The following example sets the escape character for line 1 to **!**, which is represented in the configuration file as the ASCII number 33:

```
Router(config)# line 1
Router(config-line)# escape-character !
Router(config-line)# end
Router# show running-config
Building configuration...
.
.
.
line 1
 autoselect during-login
 autoselect ppp
 modem InOut
 transport preferred none
 transport output telnet
 escape-character 33
```

Related Commands

Command	Description
show line	Displays information about the specified line connection, or all the lines.
terminal escape-character	Sets the escape character for the current terminal line for the current session.

exec

To allow an EXEC process on a line, use the **exec** command in line configuration mode. To turn off the EXEC process for the specified line, use the **no** form of this command.

exec

no exec

Syntax Description

This command has no arguments or keywords.

Defaults

The EXEC processes is enabled on all lines.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you want to allow only an outgoing connection on a line, use the **no exec** command.

The **no exec** command allows you to disable the EXEC process for connections which may attempt to send unsolicited data to the router. (For example, the control port of a rack of modems attached to an auxiliary port of router.) When certain types of data are sent to a line connection, an EXEC process can start, which makes the line unavailable.

When a user tries to Telnet to a line with the EXEC process disabled, the user will get no response when attempting to log on.

Examples

The following example disables the EXEC process on line 7.

```
Router(config)# line 7
Router(config-line)# no exec
```

exec-banner

To reenable the display of EXEC and message-of-the-day (MOTD) banners on the specified line or lines, use the **exec-banner** command in line configuration mode. To suppress the banners on the specified line or lines, use the **no** form of this command.

exec-banner

no exec-banner

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled on all lines

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command determines whether the router will display the EXEC banner and the message-of-the-day (MOTD) banner when an EXEC session is created. These banners are defined with the **banner exec** and **banner motd** global configuration commands. By default, these banner are enabled on all lines. Disable the EXEC and MOTD banners using the **no exec-banner** command.

This command has no effect on the incoming banner, which is controlled by the **banner incoming** command.

The MOTD banners can also be disabled by the **no motd-banner** line configuration command, which disables MOTD banners on a line. If the **no exec-banner** command is configured on a line, the MOTD banner will be disabled regardless of whether the **motd-banner** command is enabled or disabled. Table 31 summarizes the effects of the **exec-banner** command and the **motd-banner** command.

Table 31 Banners Displayed Based On exec-banner and motd-banner Combinations

	exec-banner (default)	**no exec-banner**
motd-banner (default)	MOTD banner EXEC banner	None
no motd-banner	EXEC banner	None

For reverse Telnet connections, the EXEC banner is never displayed. Instead, the incoming banner is displayed. The MOTD banner is displayed by default, but it is disabled if either the **no exec-banner** command or **no motd-banner** command is configured. Table 32 summarizes the effects of the **exec-banner** command and the **motd-banner** command for reverse Telnet connections.

Table 32 Banners Displayed Based On exec-banner and motd-banner Combinations for Reverse Telnet Sessions to Async Lines

	exec-banner (default)	**no exec-banner**
motd-banner (default)	MOTD banner Incoming banner	Incoming banner
no motd-banner	Incoming banner	Incoming banner

Examples

The following example suppresses the EXEC and MOTD banners on virtual terminal lines 0 to 4:

```
Router(config)# line vty 0 4
Router(config-line)# no exec-banner
```

Related Commands

Command	Description
banner exec	Defines and enables a customized banner to be displayed whenever the EXEC process is initiated.
banner incoming	Defines and enables a customized message to be displayed when there is an incoming connection to a terminal line from a host on the network.
banner motd	Defines and enables a customized message-of-the-day banner.
motd-banner	Controls (enables or disables) the display of message-of-the-day banners on a specified line or lines.

exec-character-bits

To configure the character widths of EXEC and configuration command characters, use the **exec-character-bits** command in line configuration mode. To restore the default value, use the **no** form of this command.

exec-character-bits {**7** | **8**}

no exec-character-bits

Syntax Description

7	Selects the 7-bit character set. This is the default.
8	Selects the full 8-bit character set for use of international and graphical characters in banner messages, prompts, and so on.

Defaults

7-bit ASCII character set

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Setting the EXEC character width to 8 allows you to use special graphical and international characters in banners, prompts, and so on. However, setting the EXEC character width to 8 bits can cause failures. 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.

Note If you are using the **autoselect** function, set the activation character to the default (Return) and the value for **exec-character-bits** to 7. If you change these defaults, the application will not recognize the activation request.

Examples

The following example enables full 8-bit international character sets, except for the console, which is an ASCII terminal. It illustrates use of the **default-value exec-character-bits** global configuration command and the **exec-character-bits** line configuration command.

```
Router(config)# default-value exec-character-bits 8
Router(config)# line 0
Router(config-line)# exec-character-bits 7
```

Related Commands

Command	Description
default-value exec-character-bits	Defines the EXEC character width for either 7 bits or 8 bits.
default-value special-character-bits	Configures the flow control default value from a 7-bit width to an 8-bit width.
length	Sets the terminal screen length.
terminal exec-character-bits	Locally changes the ASCII character set used in EXEC and configuration command characters for the current session.
terminal special-character-bits	Changes the ASCII character widths to accept special characters for the current terminal line and session.

exec-timeout

To set the interval that the EXEC command interpreter waits until user input is detected, use the **exec-timeout** command in line configuration mode. To remove the timeout definition, use the **no** form of this command.

exec-timeout *minutes* [*seconds*]

no exec-timeout

Syntax Description

minutes	Integer that specifies the number of minutes. The default is 10 minutes.
seconds	(Optional) Additional time intervals in seconds.

Defaults

10 minutes

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session.

To specify no timeout, enter the **exec-timeout 0 0** command.

Examples

The following example sets a time interval of 2 minutes, 30 seconds:

```
Router(config)# line console
Router(config-line)# exec-timeout 2 30
```

The following example sets a time interval of 10 seconds:

```
Router(config)# line console
Router(config-line)# exec-timeout 0 10
```

execute-on

To execute commands on a line card, use the **execute-on** command in privileged EXEC mode.

execute-on {**slot** *slot-number* | **all** | **master**} *command*

Syntax Description

slot *slot-number*	Executes the command on the line card in the specified slot. Slot numbers can be chosen from the following ranges: • Cisco 12012 router: 0 to 11 • Cisco 12008 access server: 0 to 7 • Cisco AS5800 access server: 0 to 13
all	Executes the command on all line cards.
master	(AS5800 only) Executes the designated command on a Dial Shelf Controller (DSC). Do not use this option; it is used for technical support troubleshooting only.
command	Cisco IOS command to remotely execute on the line card.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support Cisco 12000 series Gigabit Switch Routers.
11.3(2)AA	This command was implemented in images for the Cisco AS5800 series.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to execute a command on one or all line cards to monitor and maintain information on one or more line cards (for example, a line card in a specified slot on a dial shelf). This allows you to issue commands remotely; that is, to issue commands without needing to log in to the line card directly. The **all** form of the command allows you to issue commands to all the line cards without having to log in to each in turn.

Though this command does not have a **no** form, note that it is possible to use the **no** form of the remotely executed commands used in this command.

Tip This command is useful when used with **show** EXEC commands (such as **show version**), because you can verify and troubleshoot the features found only on a specific line card. Please note, however, that because not all statistics are maintained on the line cards, the output from some of the **show** commands might not be consistent.

Cisco 12000 GSR Guidelines and Restrictions

You can use the **execute-on** privileged EXEC command only from Cisco IOS software running on the GRP card.

Timesaver Though you can use the **attach** privileged EXEC command to execute commands on a specific line card, using the **execute-on slot** command saves you some steps. For example, first you must use the **attach** command to connect to the Cisco IOS software running on the line card. Next you must issue the command. Finally you must disconnect from the line card to return to the Cisco IOS software running on the GRP card. With the **execute-on slot** command, you can perform three steps with one command. In addition, the **execute-on all** command allows you to perform the same command on all line cards simultaneously.

Cisco AS5800 Guidelines and Restrictions

The purpose of the command is to conveniently enable certain commands to be remotely executed on the dial shelf cards from the router without connecting to each line card. This is the recommended procedure, because it avoids the possibility of adversely affecting a good configuration of a line card in the process. The **execute-on** command does not give access to every Cisco IOS command available on the Cisco AS5800 access server. In general, the purpose of the **execute-on** command is to provide access to statistical reports from line cards without directly connecting to the dial shelf line cards.

Caution Do not use this command to change configurations on dial shelf cards, because such changes will not be reflected in the router shelf.

Using this command makes it possible to accumulate inputs for inclusion in the **show tech-support** command.

The **master** form of the command can run a designated command remotely on the router from the DSC card. However, using the console on the DSC is *not* recommended. It is used for technical support troubleshooting only.

The **show tech-support** command for each dial shelf card is bundled into the router shelf's **show tech-support** command via the **execute-on** facility.

The **execute-on** command also support interactive commands such as the following:

```
router: execute-on slave slot slot ping
```

The **execute-on** command has the same limitations and restrictions as a **vty telnet** client has; that is, it cannot reload DSC using the following command:

```
router: execute-on slave slot slot reload
```

You can use the **execute-on** command to enable remote execution of the commands included in the following partial list:

- **debug dsc clock**
- **show context**
- **show diag**
- **show environment**
- **show dsc clock**
- **show dsi**
- **show dsip**
- **show tech-support**

Examples

In the following example, the user executes the **show controllers** command on the line card in slot 4 of a Cisco 12000 series GSR:

```
Router# execute-on slot 4 show controllers

========= Line Card (Slot 4) =======

Interface POS0
Hardware is BFLC POS
lcpos_instance struct   6033A6E0
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000400
SUNI rsop intr status   00
CRC16 enabled, HDLC enc, int clock
no loop

Interface POS1
Hardware is BFLC POS
lcpos_instance struct   6033CEC0
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000600
SUNI rsop intr status   00
CRC32 enabled, HDLC enc, int clock
no loop

Interface POS2
Hardware is BFLC POS
lcpos_instance struct   6033F6A0
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000800
SUNI rsop intr status   00
CRC32 enabled, HDLC enc, int clock
no loop

Interface POS3
Hardware is BFLC POS
lcpos_instance struct   60341E80
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000A00
SUNI rsop intr status   00
CRC32 enabled, HDLC enc, ext clock
no loop
Router#
```

Related Commands

Command	Description
attach	Connects you to a specific line card for the purpose of executing commands using the Cisco IOS software image on that line card.

exit (EXEC)

To close an active terminal session by logging off the router, use the **exit** command in EXEC mode.

exit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **exit** command in EXEC mode to exit the active session (log off the device). This command can be used in any EXEC mode (such as User EXEC mode or Privileged EXEC mode) to exit from the EXEC process.

Examples

In the following example, the **exit** (global) command is used to move from global configuration mode to privileged EXEC mode, the **disable** command is used to move from privileged EXEC mode to user EXEC mode, and the **exit** (EXEC) command is used to log off (exit the active session):

```
Router(config)# exit
Router# disable
Router> exit
```

Related Commands

Command	Description
disconnect	Disconnects a line.
end	Ends your configuration session by exiting to EXEC mode.
exit (global)	Exits from the current configuration mode to the next highest configuration mode.
logout	Closes your connection to the device (equivilant to the **exit** command).

exit (global)

To exit any configuration mode to the next highest mode in the CLI mode hierarchy, use the **exit** command in any configuration mode.

exit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

All configuration modes

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **exit** command is used in the Cisco IOS CLI to exit from the current command mode to the next highest command mode in the CLI mode hierarchy.

For example, use the **exit** command in global configuration mode to return to privileged EXEC mode. Use the **exit** command in interface, line, or router configuration mode to return to global configuration mode. Use the **exit** command in subinterface configuration mode to return to interface configuration mode. At the highest level, EXEC mode, the **exit** command will exit the EXEC mode and disconnect from the router interface (see the description of the **exit** (EXEC) command for details).

Examples

The following example shows how to exit from the subinterface configuration mode and to return to the interface configuration mode:

```
Router(config-subif)# exit
Router(config-if)#

The following example displays an exit from the interface configuration mode to return to
the global configuration mode:

Router(config-if)# exit
Router(config)#
```

Related Commands

Command	Description
disconnect	Disconnects a line.
end	Ends your configuration session by exiting to privileged EXEC mode.
exit (EXEC)	Closes the active terminal session by logging off the router.