

# L through mode

• L through mode, page 1

# L through mode

I

# length

To set the terminal screen length, use the **length** command in line configuration mode. To restore the default value, use the **no** form of this command.

length screen-length

no length

Syntax Description	screen-length		The number of lines on the screen. A value of zero disables pausing between screens of output.
Command Default	Screen length of 24 lines		
Command Modes	Line configuration		
<b>Command History</b>	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		recognize the configured sc	and to determine when to pause during multiple-screen reen length. For example, the <b>show terminal</b> command
Examples	In the following example, terminal connection on lin	•••	ed and the screen pause function is disabled for the
	Router(config)# line 6 Router(config-line)# t Router(config-line)# 1	erminal-type VT220	
<b>Related Commands</b>	Command		Description
	terminal length		Sets the number of lines on the current terminal screen for the current session.

# load-interval

To change the length of time for which data is used to compute load statistics, use the **load-interval** command in interface configuration mode or Frame Relay DLCI configuration mode. To revert to the default setting, use the **no**form of this command.

load-interval seconds

no load-interval seconds

**Syntax Description** 

*seconds* Length of time for which data is used to compute load statistics. Value is a multiple of 30, from 30 to 600 (30, 60, 90, 120, and so on). The default is 300 seconds.

Command Default Enabled

**Command Modes** Interface configuration Frame Relay DLCI configuration

<b>Command History</b>	Release	Modification
	10.3	This command was introduced.
	12.2(4)T	This command was made available in Frame Relay DLCI configuration mode.
	12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

#### **Usage Guidelines**

I

To make computations more reactive to short bursts of traffic, you can shorten the length of time over which load averages are computed.

If the load interval is set to 30 seconds, new data is used for load calculations over a 30-second period. This data is used to compute load statistics, including the input rate in bits and packets per second, the output rate in bits and packets per second, the load, and reliability.

٦

	Load data is gathered every five seconds. This data is used for a weighted-average calculation in which recent load data has more weight in the computation than older load data. If the load interval is set to 30 seconds, the average is computed for the last 30 seconds of load data. If you change the calculation interval from the default of five minutes to a shorter period of time, the input		
		rface command or the show frame-relay pvc command	
	This command is often used for dial backup purposes to of a backup interface, but it can be used on any interfa	o increase or decrease the likelihood of implementation ace.	
Examples			
Examples	In the following example, the default average of five minutes is changed to a 30-second average. A burst in traffic that would not trigger a dial backup for an interface configured with the default five-minute interval might trigger a dial backup for this interface, which is set for the shorter 30-second interval.		
	Router(config)# <b>interface serial 0</b> Router(config-if)# <b>load-interval 30</b>		
Examples	In the following example, the load interval is set to 60 seconds for a Frame Relay PVC with the DLCI 10		
	Router(config)# interface serial 1/1 Router(config-if)# frame-relay interface-dlci Router(config-fr-dlci)# load-interval 60	100	
<b>Related Commands</b>	Command	Description	

Command Description	
show interfaces     Displays statistics       router or access set	for all interfaces configured on the erver.

# location

I

To provide a description of the location of a serial device, use the <b>location</b> command in line configuration mode. To remove the description, use the <b>no</b> form of this command.		
location <i>text</i>		
no location		
text		Location description.
A location description is not provide	ed.	
Line configuration (config-line)		
Release	Modification	
10.0	This command	was introduced.
12.2(33)SRA	This command	was integrated into Cisco IOS Release 12.2(33)SRA.
The <b>location</b> command enters information about the device location and status. Use the <b>show users all</b> EXEC command to display the location information.		
In the following example, the location description for the console line is given as "Building 3, Basement":		
Router(config)# line console Router(config-line)# location Building 3, Basement		
Command		Description
show users		Displays information about the active lines on a router.
	mode. To remove the description, us         location text         no location         text         A location description is not provide         Line configuration (config-line)         Release         10.0         12.2(33)SRA         The location command enters inform command to display the location inf         In the following example, the location         Router (config) # line console Router (config-line) # location         Command	mode. To remove the description, use the no form of         location text         no location         text         A location description is not provided.         Line configuration (config-line)         Release       Modification         10.0       This command         12.2(33)SRA       This command         The location command enters information about the d command to display the location information.         In the following example, the location description for         Router (config=line) # location Building 3, Base         Command

I

٦

# lock

	To configure a temporary password on a line, use the <b>lock</b> command in EXEC mode.	
	lock	
Syntax Description	This command has no argun	nents or keywords.
Command Default	Not locked	
Command Modes	EXEC	
Command History	Release	Modification
	10.0	This command was introduced in a release prior to Cisco IOS Release 10.0.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Usage Guidelines	<ul> <li>You can prevent access to your session while keeping your connection open by setting up a temporary password.</li> <li>1 Enter the lock command. The system prompts you for a password.</li> <li>2 Enter a password, which can be any arbitrary string. The system will prompt you to confirm the password. The screen then clears and displays the message "Locked."</li> <li>3 To regain access to your sessions, reenter the password.</li> <li>The Cisco IOS software honors session timeouts on a locked lines. You must clear the line to remove this feature. The system administrator must set the line up to allow use of the temporary locking feature by usin the lockable line configuration command.</li> </ul>	
Examples	The following example shows configuring the router as lockable, saving the configuration, and then locking the current session for the user: Router(config-line)# lockable Router(config-line)# ^Z Router# copy system:running-config nvram:startup-config Building configuration OK Router# lock Password: <password> Locked Password: <password> Router#</password></password>	

#### **Related Commands**

I

Command	Description
lockable	Enables the lock EXEC command.
login (EXEC)	Enables or changes a login username.

I

setting a temporary password on your terminal line.

1

# lockable

	To enable use of the <b>lock</b> EXEC command, use the <b>lockable</b> command in line configuration mode. To reinstate the default (the terminal session cannot be locked), use the <b>no</b> form of this command.		
	lockable no lockable		
Syntax Description	This command has no arguments or keywords.		
Command Default	Sessions on the line are not lockable (the lock EXEC command has no effect).		
Command Modes	Line configuration		
Command History	Release	Modification	
	10.0	This command y	was introduced.
	12.2(33)SRA	This command w	was integrated into Cisco IOS Release 12.2(33)SRA.
Usage Guidelines			ing, which is executed using the <b>lock</b> EXEC command. on open while preventing access by other users.
Examples	In the following example, the terminal connection is configured as lockable, then the current connection is locked:		
	Router# configure terminal Router(config)# line consol Router(config-line)# lockat Router(config)# ^Z Router# lock Password: <password> Again: <password> Locke</password></password>	ble	
	Password: <b><password></password></b> Router#		
Related Commands	Command		Description
	lock		Prevents access to your session by other users by

# log config

To enter configuration change logger configuration mode, use the **log config**command in archive configuration mode.

log config

- **Syntax Description** This command has no arguments or keywords.
- **Command Default** Configuration change logger configuration mode is not entered.
- **Command Modes** Archive configuration (config-archive)

**Command History** Release Modification 12.3(4)T This command was introduced. This command was integrated into Cisco IOS Release 12.2(25)S. 12.2(25)S 12.2(27)SBC This command was integrated into Cisco IOS Release 12.2(27)SBC. This command was integrated into Cisco IOS Release 12.2(33)SRA. 12.2(33)SRA 12.2(33)SB This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series. Cisco IOS XE Release 3.9S This command was integrated into Cisco IOS XE Release 3.9S.

#### **Examples**

The following example shows how to place the device in configuration change logger configuration mode:

Device# configure terminal
!
Device(config)# archive
Device(config-archive)# log config
Device(config-archive-log-config)#

Related Commands	Command	Description
	archive	Enters archive configuration mode.
	hidekeys	Suppresses the display of password information in configuration log files.
	logging enable	Enables the logging of configuration changes.

٦

Command	Description
logging size	Specifies the maximum number of entries retained in the configuration log.
notify syslog	Enables the sending of notifications of configuration changes to a remote syslog.
show archive log config	Displays entries from the configuration log.

# logging buginf

To allow debug messages to be generated for the standard system logging buffer, use the logging **buginf** command in global configuration mode. To disable the logging for debugging functionality, use the no form of this command. logging buginf no logging buginf **Syntax Description** This command has no arguments or keywords. **Command Default** Debug messages are not suppressed. **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)SRC This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. 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. **Usage Guidelines** The **no logging buginf** command is used to avoid a situation where a large amount of debug messages might overload the processor (CPU hog condition). This condition differs from the use of the undebug allcommand wherein all debugging calls are disabled in the Cisco IOS software. No debug reporting is available, even if debugging is enabled. Note that even though debugging has been completely disabled in the system, other message reporting, including error reporting, is still available. **Examples** The following example shows how to enable buginf logging for debugging:

Router# configure terminal Router(config)# logging buginf

٦

#### **Related Commands**

Command	Description
show logging	Displays the state of system logging (syslog) and the contents of the standard system logging buffer.

# logging enable

To enable the logging of configuration changes, use the **logging enable** command in configuration change logger configuration mode. To disable the logging of configuration changes, use the **no** form of this command.

logging enable

no logging enable

- **Syntax Description** This command has no arguments or keywords.
- **Command Default** Configuration change logging is disabled.

**Command Modes** Configuration change logger configuration (config-archive-log-config)

Command History	Release	Modification
	12.3(4)T	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.
	Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

**Usage Guidelines** Use this command if you want to log configuration changes. If you disable configuration logging, all configuration log records that were collected are purged.

**Examples** 

The following example shows how to enable configuration logging:

Device# configure terminal
!
Device(config)# archive
Device(config-archive)# log config
Device(config-archive-log-config)# logging enable
Device(config-archive-log-config)# end
The following example shows how to clear the configuration log by disabling and then reenabling the
configuration log:

Device# configure terminal

```
!
Device(config)# archive
Device(config-archive)# log config
Device(config-archive-log-config)# no logging enable
Device(config-archive-log-config)# logging enable
Device(config-archive-log-config)# end
```

#### **Related Commands**

Command	Description
archive	Enters archive configuration mode.
hidekeys	Suppresses the display of password information in configuration log files.
log config	Enters configuration change logger configuration mode.
logging size	Specifies the maximum number of entries retained in the configuration log.
notify syslog	Enables the sending of notifications of configuration changes to a remote syslog.
show archive log config	Displays entries from the configuration log.

# logging esm config

To permit configuration changes from Embedded Syslog Manager (ESM) filters, use the **logging esm config** command in global configuration mode. To disable the configuration, use the **no** form of this command.

logging esm config

no logging esm config

- **Syntax Description** This command has no arguments or keywords.
- **Command Default** ESM filters are enabled.
- **Command Modes** Global configuration (config)

<b>Command History</b>	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)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
	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.

**Usage Guidelines** You can use the **no logging esm config** command to disallow configuration changes from ESM filters.

**Examples** The following example shows how to configure the ESM filters:

Router# configure terminal Router(config)# logging esm config

#### **Related Commands**

I

Command	Description
logging filter	Specifies a syslog filter module to be used by the ESM.

Cuntary Decemintian

# logging event bundle-status

To enable message bundling, use the **logging event bundle-status** command in interface configuration mode. To disable message bundling, use the **no** form of this command.

#### logging event bundle-status

no logging event bundle-status

Syntax Description	default	Enables system logging of interface state-change events on all interfaces in the system.
	boot	Enables system logging of interface state-change events on all interfaces in the system during system initialization.

- **Command Default** Message bundling does not occur.
- **Command Modes** Global configuration

<b>Command History</b>	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 logging event bundle-status command is not applicable on Port Channel or Ether-Channel interfaces.

**Examples** This example shows how to enable the system logging of the interface state-change events on all interfaces in the system:

Router(config)# logging event bundle-status
Router(config)# end
Router # show logging event bundle-status
\*Aug 4 17:36:48.240 UTC: %EC-SP-5-UNBUNDLE: Interface FastEthernet9/23 left the port-channel
Port-channel2
\*Aug 4 17:36:48.256 UTC: %LINK-SP-5-CHANGED: Interface FastEthernet9/23, changed state to
administratively down
\*Aug 4 17:36:47.865 UTC: %EC-SPSTBY-5-UNBUNDLE: Interface FastEthernet9/23 left the
port-channel Port-channel2
Router # show logging event bundle-status

\*Aug 4 17:37:35.845 UTC: %EC-SP-5-BUNDLE: Interface FastEthernet9/23 joined port-channel
Port-channel2
\*Aug 4 17:37:35.533 UTC: %EC-SPSTBY-5-BUNDLE: Interface FastEthernet9/23 joined port-channel
Port-channel2

#### **Related Commands**

I

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

# logging event link-status (global configuration)

To change the default or set the link-status event messaging during system initialization, use the **logging event link-status** command in global configuration mode. To disable the link-status event messaging, use the **no** form of this command.

logging event link-status {default| boot}

no logging event link-status {default| boot}

Syntax Description	default	Enables system logging of interface state-change events on all interfaces in the system.
	boot	Enables system logging of interface state-change events on all interfaces in the system during system initialization.

- **Command Default** Interface state-change messages are not sent.
- **Command Modes** Global configuration

<b>Command History</b>	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**

You do not have to enter the **logging event link-status boot** command to enable link-status messaging during system initialization. The **logging event link-status default** command logs system messages even during system initialization.

If you enter both the **logging event link-status default** and the **no logging event link-status boot**commands, the interface state-change events are logged after all modules in the Cisco 7600 series router come online after system initialization. The **logging event link-status default** and the **no logging event link-status boot** commands are saved and retained in the running configuration of the system.

When both the **logging event link-status default** and the **no logging event link-status boot**commands are present in the running configuration and you want to display the interface state-change messages during system initialization, enter the **logging event link-status boot** command.

**Examples** This example shows how to enable the system logging of the interface state-change events on all interfaces in the system:

Router (config) # logging event link-status default Router (config) # This example shows how to enable the system logging of interface state-change events on all interfaces during system initialization:

Router(config) # logging event link-status boot Router(config) # This example shows how to disable the system logging of interface state-change events on all interfaces:

Router (config) # no logging event link-status default Router (config) # This example shows how to disable the system logging of interface state-change events during system initialization:

```
Router(config)# no logging event link-status boot
Router(config)#
```

#### **Related Commands**

I

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

## logging event link-status (interface configuration)

To enable link-status event messaging on an interface, use the **logging event link-status** command in interface configuration mode. To disable link-status event messaging, use the **no** form of this command.

logging event link-status [bchan| dchan| nfas]

no logging event link-status [bchan| dchan| nfas]

Syntax	Des	cription
• ]		0

bchan	(Optional) Logs B-channel status messages. This keyword is available only for integrated services digital network (ISDN) serial interfaces.
dchan	(Optional) Logs D-channel status messages. This keyword is available only for ISDN serial interfaces.
nfas	(Optional) Logs non-facility associated signaling (NFAS) D-channel status messages. This keyword is available only for ISDN serial interfaces.

Command Default	Interface state-change messages are not sent.
-----------------	---

**Command Modes** Interface configuration (config-if)

<b>Command History</b>	Release	Modification
	12.2(14)SX	This command was introduced on the Supervisor Engine 720.
	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.

**Usage Guidelines** To enable system logging of interface state-change events on a specific interface, enter the **logging event link-status** command.

**Examples** The following example shows how to enable link-status event messaging on an interface:

Router(config-if) # logging event link-status This example shows how to disable link-status event messaging on an interface:

Router(config-if) # no logging event link-status

## logging event subif-link-status

To enable the link-status event messaging on a subinterface, use the **logging event subif-link-status** command in interface configuration mode. To disable the link-status event messaging on a subinterface, use the **no** form of this command.

logging event subif-link-status no logging event subif-link-status

- **Syntax Description** This command has no arguments or keywords.
- **Command Default** Subinterface state-change messages are not sent.
- **Command Modes** Interface configuration

<b>Command History</b>	Release	Modification
	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 is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720. To enable system logging of interface state-change events on a specific subinterface, enter the logging event subif-link-status command. To enable system logging of interface state-change events on a specific interface, enter the logging event link-status command. To enable system logging of interface state-change events on all interfaces in the system, enter the logging event link-status command. **Examples** This example shows how to enable the system logging of the interface state-change events on a subinterface: Router(config-if) # logging event subif-link-status Router(config-if)# This example shows how to disable the system logging of the interface state-change events on a subinterface: Router(config-if) # no logging event subif-link-status Router(config-if)#

٦

#### **Related Commands**

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

### logging event trunk-status

To enable trunk status messaging, use the **logging event trunk-status** command in interface configuration mode. To disable trunk status messaging, use the **no** form of this command.

logging event trunk-status

no logging event trunk-status

- **Syntax Description** This command has no keywords or variables.
- **Command Default** This command has no default settings.
- **Command Modes** Interface configuration mode

<b>Command History</b>	Release	Modification
	12.2(14)SX	Support for this command was introduced.

**Usage Guidelines** The logging event bundle-status command is not applicable on Port Channel or Ether-Channel interfaces.

**Examples** This example shows how to enable the trunk status messaging on physical ports:

Router(config)# logging event trunk-status Router(config)# end Router# show logging event trunk-status \*Aug 4 17:27:01.404 UTC: %DTP-SPSTBY-5-NONTRUNKPORTON: Port Gi3/3 has become non-trunk \*Aug 4 17:27:00.773 UTC: %DTP-SP-5-NONTRUNKPORTON: Port Gi3/3 has become non-trunk Router#

# logging reload

To set the reload logging level, use the **logging reload** command in global configuration mode. To disable the reload logging, use the **no** form of this command.

logging reload [message-limit *number*] [severity-level| alerts| critical| debugging| emergencies| errors| informational| notifications| warnings]

no logging reload

#### **Syntax Description**

message-limit	(Optional) Sets the limit on the number of messages that can be logged during reload.
number	Number of messages. The range is from 1 to 4294967295.
severity-level	(Optional) Logging severity level. The range is from 0 to 7.
alerts	(Optional) Specifies that an immediate action is needed.
critical	(Optional) Specifies the critical conditions.
debugging	(Optional) Displays the debugging messages
emergencies	(Optional) Specifies that the system is unusable.
errors	(Optional) Specifies error conditions
informational	(Optional) Specifies error informational messages
notifications	(Optional) Specifies normal but significant conditions.
warnings	(Optional) Specifies warning conditions.

#### **Command Default** The logging reload message limit is 1000 notifications.

#### **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.

ſ

	Release	Modification	
	12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.	
	12.2(33)SXI	This command wa Release 12.2(33)S	as integrated into a release earlier than Cisco IOS SXI.
	Cisco IOS XE Releas e2.1	This command wa	as integrated into Cisco IOS XE Release 2.1.
Usage Guidelines	The default setting is recommended. Setting the message-limit too low may result in losing important message during reload. If the <b>logging reload</b> command is not enabled, logging is turned off during reload.		
Examples	The following example shows how to set the limit on number of messages that can be logged during reloa to 100:		
	Router# <b>configure terminal</b> Router(config)# <b>logging reload message-limit 100</b>		
<b>Related Commands</b>	Command		Description
	show logging		Displays the state of system logging (syslog) and the contents of the standard system logging buffer.

# logging ip access-list cache (global configuration)

To configure the Optimized ACL Logging (OAL) parameters, use the **logging ip access-list cache** command in global configuration mode. To return to the default settings, use the **no** form of this command.

logging ip access-list cache {entries entries interval seconds rate-limit pps threshold packets}

no logging ip access-list cache [entries| interval| rate-limit| threshold]

#### **Syntax Description**

entries entries	Specifies the maximum number of log entries that are cached in the software; valid values are from 0 to 1048576 entries.
interval seconds	Specifies the maximum time interval before an entry is sent to syslog; valid values are from 5 to 86400 seconds.
rate-limit pps	Specifies the number of packets that are logged per second in the software; valid values are from 10 to 1000000 pps.
threshold packets	Specifies the number of packet matches before an entry is sent to syslog; valid values are from 1 to 1000000 packets.

#### **Command Default** The defaults are as follows:

- entries --8000 entries.
- seconds --300 seconds (5 minutes).
- rate-limit *pps* --0 (rate limiting is off) and all packets are logged.
- **threshold** *packets* --**0** (rate limiting is off) and the system log is not triggered by the number of packet matches.

#### **Command Modes** Global configuration

<b>Command History</b>	Release	Modification
	12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

**Usage Guidelines** 

only.

	OAL is supported on IPv4 unicast traffic only.			
	You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible With OAL configured, use SPAN to capture traffic.			
	If the entry is inactive for the duration that is specified in the <b>update-interval</b> seconds command, the entry is removed from the cache.			
	If you enter the <b>no logging ip access-list cache</b> comm to the default values.	and without keywords, all the parameters are returned		
	You must set ICMP unreachable rate limiting to 0 if the	e OAL is configured to log denied packets.		
	When enabling the IP "too short" check using the mls verify ip length minimum command, valid IP packets with with an IP protocol field of ICMP(1), IGMP(2), IP(4), TCP(6), UDP(17), IPv6(41), GRE(47), or SIPP-ESP(50) will be hardware switched. All other IP protocol fields are software switched.			
$\triangle$				
	Using optimized access-list logging (OAL) and the mls verify ip length minimum command together can cause routing protocol neighbor flapping as they are incompatible			
Examples	This example shows how to specify the maximum number of log entries that are cached in the software Router(config)# logging ip access-list cache entries 200 This example shows how to specify the maximum time interval before an entry is sent to the system log			
	Router (config) # logging ip access-list cache interval 350 This example shows how to specify the number of pac	ckets that are logged per second in the software:		
	Router(config) # logging ip access-list cache rate-limit 100 This example shows how to specify the number of pac	eket matches before an entry is sent to the system log:		
	Router(config)# logging ip access-list cache threshold 125			
<b>Related Commands</b>	Command	Description		
	clear logging ip access-list cache	Clears all the entries from the OAL cache and sends them to the syslog.		

logging ip access-list cache (interface

configuration)

I

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720

is based on direction.

Enables an OAL-logging cache on an interface that

٦

Command	Description
update-interval seconds	Removes entries from the cache that are inactive for the duration that is specified in the command.

I

# logging ip access-list cache (interface configuration)

To enable an Optimized ACL Logging (OAL)-logging cache on an interface that is based on direction, use the **logging ip access-list cache** command in interface configuration mode. To disable OAL, use the **no** form of this command.

logging ip access-list cache [in| out]

no logging ip access-list cache

Syntax Description	in	(Optional) Enables OAL on ingress packets.	
	out	(Optional) Enables OAL on egress packets.	
Command Default	Disabled		
Command Modes	Interface configuration		
Command History	Release	Modification	
	12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.	
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.	
Usage Guidelines	This command is supported on Cisc only.	to 7600 series routers that are configured with a Supervisor Engine 720	
	This command is supported on traffic that matches the <b>log</b> keyword in the applied ACL. You muunreachable rate limiting to 0 if the OAL is configured to log denied packets.		
On systems that are configured with a PFC3A, support for the egress direction on tu supported.		a PFC3A, support for the egress direction on tunnel interfaces is not	
	OAL is supported on IPv4 unicast traffic only.		
	You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.		
	If the entry is inactive for the duration that is specified in the <b>update-interval</b> <i>seconds</i> command, the entry is removed from the cache.		
	If you enter the <b>no logging ip acces</b> to the default values.	s-list cache command without keywords, all the parameters are returned	

When enabling the IP "too short" check using the mls verify ip length minimum command, valid IP packets with with an IP protocol field of ICMP(1), IGMP(2), IP(4), TCP(6), UDP(17), IPv6(41), GRE(47), or SIPP-ESP(50) will be hardware switched. All other IP protocol fields are software switched.

**Caution** Using optimized access-list logging (OAL) and the mls verify ip length minimum command together can cause routing protocol neighbor flapping as they are incompatible

#### **Examples**

This example shows how to enable OAL on ingress packets:

Router(config-if)# logging ip access-list cache in This example shows how to enable OAL on egress packets:

Router(config-if)#
logging ip access-list cache out

#### **Related Commands**

Command	Description
clear logging ip access-list cache	Clears all the entries from the OAL cache and sends them to the syslog.
logging ip access-list cache (global configuration)	Configures the OAL parameters.
show logging ip access-list	Displays information about the logging IP access list.
update-interval seconds	Removes entries from the cache that are inactive for the duration that is specified in the command.

# logging persistent (config-archive-log-cfg)

To enable the configuration logging persistent feature and to select how the configuration commands are to be saved to the Cisco IOS secure file system, use the **logging persistent** command in the log config submode of archive configuration mode. To disable this capability, use the **no** form of this command.

logging persistent {auto| manual}

no logging persistent {auto| manual}

Syntax Description	auto	Specifies that each configuration command will be saved automatically to the Cisco IOS secure file system.
	manual	Specifies that each configuration command must be saved manually to the Cisco IOS secure file system.

**Command Default** The configuration commands are not saved to the Cisco IOS secure file system.

**Command Modes** Archive configuration mode, log config (configuration-change logger) submode (config-archive-log-cfg)#

<b>Command History</b>	Release	Modification
	12.0(26)S	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

#### **Usage Guidelines**

I

When you use the **manual**keyword, you must save each configuration command manually to the Cisco IOS secure file system. To do this, you must use the **archive log config persistent save** command.

#### **Examples**

The following example automatically saves the configuration commands to the Cisco IOS secure file system:

```
Router(config)# archive
Router(config-archive)# log config
Router(config-archive-log-cfg)# logging enable
Router(config-archive-log-cfg)# logging persistent auto
```

#### **Related Commands**

Command	Description
logging persistent reload	Sequentially applies configuration commands in the configuration logger database to the running-config file after a reload.
archive log config persistent save	Saves the persisted commands in the configuration log to the Cisco IOS secure file system.

# logging persistent reload (config-archive-log-cfg)

To sequentially apply the configuration commands saved in the configuration logger database (since the last **write memory**command) to the running-config file after a reload, use the **logging persistent reload** command in configuration change logger configuration mode in archive configuration mode. To disable this capability, use the **no** form of this command.

logging persistent reload no logging persistent reload

- **Syntax Description** This command has no arguments or keywords.
- **Command Default** The configuration commands saved in the configuration logger database are not applied to the running-config file.

**Command Modes** Archive config mode; log config (configuration change logger) submode (config-archive-log-cfg)#

<b>Command History</b>	Release	Modification
	12.2(33)SRA	This command was introduced.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines	Use the logging persistent reload command when you want changed configuration commands to take effect
	on the next reload of the router.

**Examples** The following example applies the configuration commands in the configuration logger database to the running-config file after the next reload:

Router(config-archive-log-cfg)# logging persistent reload

<b>Related Commands</b>	Command	Description
	logging persistent	Enables the configuration logging persistent feature.

# logging size

To specify the maximum number of entries retained in the configuration log, use the **logging size** command in configuration change logger configuration mode. To reset the default value, use the **no** form of this command.

logging size entries

no logging size

Syntax Description	entries	The maximum number of entries retained in the configuration log. Valid values range from 1 to 1000. The default value is 100 entries.
		configuration log. Valid values range from 1 to 10

**Command Default** 100 entries

**Command Modes** Configuration change logger configuration (config-archive-log-config)

<b>Command History</b>	Release	Modification
	12.3(4)T	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.
	Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

#### **Usage Guidelines**



When the configuration log is full, the oldest log entry is removed every time a new entry is added.

If a new log size is specified that is smaller than the current log size, the oldest entries will be immediately purged until the new log size is satisfied, regardless of the age of the log entries.

#### **Examples**

The following example shows how to specify that the configuration log may have a maximum of 200 entries:

Device (config-archive-log-config) # **logging size 200** The following example shows how to clear the configuration log by reducing the log size to 1, then resetting the log size to the desired value. Only the most recent configuration log file will be saved.

```
Device(config)# archive
Device(config-archive)# log config
Device(config-archive-log-config)# logging size 1
Device(config-archive-log-config)# logging size 200
```

#### **Related Commands**

I

Command	Description
archive	Enters archive configuration mode.
hidekeys	Suppresses the display of password information in configuration log files.
log config	Enters configuration change logger configuration mode.
logging enable	Enables the logging of configuration changes.
notify syslog	Enables the sending of notifications of configuration changes to a remote syslog.
show archive log config	Displays entries from the configuration log.

# logging synchronous

To synchronize unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty, use the **logging synchronous** command in line configuration mode. To disable synchronization of unsolicited messages and debug output, use the **no** form of this command.

logging synchronous [level severity-level| all] [limit number-of-lines] no logging synchronous [level severity-level| all] [limit number-of-lines]

#### **Syntax Description**

IUN	level severity-level	(Optional) Specifies the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. Low numbers indicate greater severity and high numbers indicate lesser severity. The default value is 2.
	all	(Optional) Specifies that all messages are printed asynchronously, regardless of the severity level.
	limit number-of-lines	(Optional) Specifies the number of buffer lines to be queued for the terminal, after which new messages are dropped. The default value is 20.

# Command DefaultThis command is disabled.If you do not specify a severity level, the default value of 2 is assumed.If you do not specify the maximum number of buffers to be queued, the default value of 20 is assumed.

#### **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.	
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**

When synchronous logging of unsolicited messages and debug output is turned on, unsolicited Cisco IOS software output is displayed on the console or printed after solicited Cisco IOS software output is displayed or printed. This keeps unsolicited messages and debug output from being interspersed with solicited software output and prompts.

Tip

This command is useful for keeping system messages from interrupting your typing. By default, messages will appear immediately when they are processed by the system, and the CLI cursor will appear at the end of the displayed message. For example, the line "Configured by console from console" may be printed to the screen, interrupting whatever command you are currently typing. The **logging synchronous** command allows you to avoid these potentially annoying interruptions without have to turn off logging to the console entirely.

When this command is enabled, unsolicited messages and debug output are displayed on a separate line than user input. After the unsolicited messages are displayed, the CLI returns to the user prompt.

Note

This command is also useful for allowing you to continue typing when debugging is enabled.

When specifying a severity level number, consider that for the logging system, low numbers indicate greater severity and high numbers indicate lesser severity.

When a message queue limit of a terminal line is reached, new messages are dropped from the line, although these messages might be displayed on other lines. If messages are dropped, the notice "%SYS-3-MSGLOST *number-of-messages* due to overflow" follows any messages that are displayed. This notice is displayed only on the terminal that lost the messages. It is not sent to any other lines, any logging servers, or the logging buffer.

Caution

By configuring abnormally large message queue limits and setting the terminal to "terminal monitor" on a terminal that is accessible to intruders, you expose yourself to "denial of service" attacks. An intruder could carry out the attack by putting the terminal in synchronous output mode, making a Telnet connection to a remote host, and leaving the connection idle. This could cause large numbers of messages to be generated and queued, and these messages could consume all available RAM. You should guard against this type of attack through proper configuration.

#### **Examples**

In the following example, a system message appears in the middle of typing the show running-config command:

```
Router(config-line)# end
Router# show ru
2w1d: %SYS-5-CONFIG_I: Configured from console by consolenning-config
.
.
```

The user then enables synchronous logging for the current line (indicated by the \* symbol in the **show line** command), after which the system displays the system message on a separate line, and returns the user to the prompt to allow the user to finish typing the command on a single line:

```
Router# show line
```

Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int \* 0 CTY 0 0/0 3 -Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)# line 0 Router(config-line) # logging syn <tab> Router(config-line) # logging synchronous Router(config-line) # end Router# show ru 2w1d: %SYS-5-CONFIG I: Configured from console by console Router# show running-config In the following example, synchronous logging for line 4 is enabled with a severity level of 6. Then synchronous logging for line 2 is enabled with a severity level of 7 and is specified with a maximum number of buffer lines of 1,000.

```
Router(config)# line 4
Router(config-line)# logging synchronous level 6
Router(config-line)# exit
Router(config)# line 2
Router(config-line)# logging synchronous level 7 limit 1000
Router(config-line)# end
Router#
```

Command	Description
line	Identifies a specific line for configuration and starts the line configuration command collection mode.
logging on	Controls logging of error messages and sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

# logging system

To enable System Event Archive (SEA) logging, use the **logging system**command in global configuration mode. To disable SEA logging, use the **no** form of this command.

logging system [disk name]

no logging system

Syntax Description	disk name	(Optional) Stores the system event archive (system
		event log file) in the specified disk. The specified disk
		must be already have been configured to allow for
		the storage of the system event archive.

**Command Default** By default, SEA logging feature is enabled, and the events are logged to a file on a persistent storage device (bootflash: or disk:).

## **Command Modes** Global configuration (config)

<b>Command History</b>	Release	Modification
	12.2(33)SXH	This command was introduced.
	12.2(33)SCC	The command was introduced for the Cisco uBR10012 router in the Cisco IOS Software Release 12.2(33)SCC.

#### **Usage Guidelines**

SEA is supported on switches that have a Supervisor Engine 32 or Supervisor Engine 720 with a compact flash adapter and a Compact Flash card (WS-CF-UPG= for Supervisor Engine 720).

To stop SEA logging to a specified disk, use the default logging system command.

For documentation of the configuration tasks associated with this feature, see the chapter "Configuring the System Event Archive" in the Catalyst 6500 Release 12.2SX Software Configuration Guide .

#### **Cisco Universal Broadband Router 100112**

The SEA feature is used to address the deficiencies of the debug trace and system console. Support for SEA feature was introduced on Cisco uBR10012 Router in the Cisco IOS Release 12.2(33)SCC. Use the **logging** system disk command to change the location of the disk used to store the sea\_log.dat file.

Note

To store the system event logs, the SEA requires either PCMCIA ATA disk or Compact Flash disk in compact flash adapter for PRE2.

# **Examples** The following example shows how to specify that the SEA log file should be written to the disk "disk1:":

Router(config) # logging system disk disk1:

Router(config)# end

clear logging system	Clears the event records stored in the SEA.
copy logging system	Copies the archived system event log to another location.
show logging system	Displays the SEA logging system disk.

# logout

	To close an active terminal session by logging off the router, use the <b>logout</b> command in user EXEC mode.		
	logout		
Syntax Description	This command has no arguments of	or keywords.	
Command Default	No default behavior or values.		
Command Modes	User 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.	

**Examples** 

I

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 **logout** command is used to log off (exit from the active session):

Router(config)# **exit** Router# **disable** Router> **logout** 

# logout-warning

To warn users of an impending forced timeout, use the **logout-warning**command in line configuration mode. To restore the default, use the **no** form of this command.

logout-warning [ seconds ]

logout-warning

Syntax Description	seconds		(Optional) Number of seconds that are counted down before session termination. If no number is specified, the default of 20 seconds is used.
Command Default	No warning is sent to the user.		
Command Modes	Line configuration		
Command History	Release	Modification	
	10.3	This command	was introduced.
	12.2(33)SRA	This command	was integrated into Cisco IOS Release 12.2(33)SRA.
Usage Guidelines Examples		varning is configu	ed timeout (set using the <b>absolute-timeout</b> command). ared on line 5 with a countdown value of 30 seconds:
<b>Related Commands</b>	Command		Description
	absolute-timeout		Sets the interval for closing user connections on a specific line or port.
	session-timeout		Sets the interval for closing the connection when there is no input or output traffic.

# macro (global configuration)

To create a global command macro, use the **macro**command in global configuration mode. To remove the macro, use the **no** form of this command.

**macro** {**global** {**apply** *macro-name*| **description** *text*| **trace** *macro-name* [ *keyword-to-value* ] *value-first-keyword* [ *keyword-to-value* ] *value-second-keyword* [ *keyword-to-value* ] *value-third-keyword* [ *keyword-to-value* ]}| **name** *macro-name*}

**no macro** {**global** {**apply** *macro-name*| **description** *text*| **trace** *macro-name* [ *keyword-to-value* ] *value-first-keyword* [ *keyword-to-value* ] *value-second-keyword* [ *keyword-to-value* ] *value-third-keyword* [ *keyword-to-value* ]}| **name** *macro-name*}

### **Syntax Description**

global	Applies the macro globally.
apply macro-name	Applies a specified macro.
description text	Provides a description of the macros applied to the switch.
trace macro-name	Applies a specified macro with trace enabled.
keyword-to-value	(Optional) Keyword to replace with a value.
value-first-keyword	Value of the first keyword to replace.
value-second-keyword	Value of the second keyword to replace.
value-third-keyword	Value of the third keyword to replace.
name macro-name	Specifies the name of a macro.

### **Command Default** This command has no default setting.

**Command Modes** Global configuration (config)

### **Command History**

Release	Modification	
12.2(33)SXH	This command was introduced.	
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.	

#### Usage Guidelines

You can enter up to three keyword pairs using the **macro global trace** command.

You can enter the **macro global description** command on the switch stack or on a standalone switch.

Use the **description** *text*keyword and argument to associate the comment text, or the macro name with a switch. When multiple macros are applied on a switch, the description text is used from the last applied macro. You can verify the global description settings by using the **show parser macro description** command.

To find the syntax or configuration errors, enter the **macro global trace** *macro-name* command to apply and debug the macro.

To display a list of any keyword-value pairs defined in the macro, enter the **macro global apply** *macro-name* ? command.

You can delete a global macro-applied configuration on a switch only by entering the **no** version of each command that is in the macro.

Keyword matching is case sensitive.

When a macro is applied on the commands, all matching occurrences of keywords are replaced with the corresponding values.

The **no** form of the **macro name** command deletes only the macro definition. It does not affect the configuration of the interfaces on which the macro is already applied.

**Examples** The following example shows how to apply the macro called snmp to set the hostname address to "test-server" and to set the IP precedence value to 7:

Router (config) # macro global apply snmp ADDRESS test-server VALUE 7 The following example shows how to debug the macro called snmp by using the macro global trace command to find the syntax or configuration errors in the macro when it is applied to a switch:

```
Router(config) # macro global trace snmp VALUE 7 VALUE 8 VALUE 9
Applying command...`snmp-server enable traps port-security'
Applying command...`snmp-server enable traps linkup'
Applying command...`snmp-server nable traps linkdown'
Applying command...`snmp-server host'
%Error Unknown error.
Applying command...`snmp-server ip precedence 7'
Router(config)#
```

Command	Description
macro (interface configuration)	Creates an interface-specific command macro.
show parser macro	Displays the smart port macros.

# macro (interface configuration)

To create an interface-specific command macro, use the **macro** command in interface configuration mode. To remove the macro, use the **no** form of this command.

**macro** {**apply** *macro-name*| **description** *text*| **trace** *macro-name* [ *keyword-to-value* ] *value-first-keyword* [ *keyword-to-value* ] *value-second-keyword* [ *keyword-to-value* ] *value-third-keyword* [ *keyword-to-value* ] }

**no macro** {**apply** *macro-name*| **description** *text*| **trace** *macro-name* [*keyword-to-value*] *value-first-keyword* [*keyword-to-value*] *value-second-keyword* [*keyword-to-value*] *value-third-keyword* [*keyword-to-value*]}

#### **Syntax Description**

apply macro-name	Applies a specified macro.
description text	Specifies a description about the macros that are applied to the interface.
trace macro-name	Applies a specified macro with trace enabled.
keyword-to-value	(Optional) Keyword to replace with a value.
value-first-keyword	Value of the keyword to replace.

#### **Command Default** This command has no default setting.

**Command Modes** Interface configuration (config-if)

<b>Command History</b>	Release	Modification
	12.2(33)SXH	This command was introduced.

#### Usage Guidelines

elines You can enter up to three keyword changes using the macro trace command.

You can enter the macro description command on the switch stack or on a standalone switch.

Use the **description** *text* keyword and argument to associate comment text, or the macro name, with a switch. When multiple macros are applied on a switch, the description text will be from the last applied macro. You can verify the **description** settings by entering the **show parser macro description** command.

To find any syntax or configuration errors, enter the **macro trace** *macro-name* command to apply and debug the macro.

To display a list of any keyword-value pairs defined in the macro, enter the **macro apply** *macro-name* ? command.

To successfully apply the macro, you must enter any required keyword-value pairs.

Keyword matching is case sensitive.

In the commands that the macro applies, all matching occurrences of keywords are replaced with the corresponding values.

You can delete all configuration on an interface by entering the **default interface** *interface* interface configuration command.

**Examples** The following example shows how to apply the user-created macro called desktop-config and to verify the configuration:

Router(config) # interface fastethernet1/2

Router(config-if) # macro apply desktop-config

The following example shows how to apply the user-created macro called desktop-config and to replace all occurrences of vlan with VLAN ID 25:

Router(config-if) # macro apply desktop-config vlan 25

Command	Description
macro (global configuration)	Creates a command macro.
show parser macro	Displays the smart port macros.

# maximum

To set the maximum number of archive files of the running configuration to be saved in the Cisco configuration archive, use the **maximum** command in archive configuration mode. To reset this command to its default, use the **no** form of this command.

maximum number

no maximum number

**Syntax Description** 

I

number

Maximum number of archive files of the running configuration to be saved in the Cisco configuration archive. You can archive from 1 to 14 configuration files. The default is 10.

**Command Default** By default, a maximum of 10 archive files of the running configuration are saved in the Cisco configuration archive.

**Command Modes** Archive configuration (config-archive)

<b>Command History</b>	Release	Modification
	12.3(7)T	This command was introduced.
	12.2(25)8	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(31)SB2	This command was implemented on the Cisco 10000 series.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.
	Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.98.



Note

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

After the maximum number of files are saved in the Cisco configuration archive, the oldest file is automatically deleted when the next, most recent file is saved.

N. Note

This command should only be used when a local writable file system is specified in the *url* argument of the **path** command. Network file systems may not support deletion of previously saved files.

**Examples** 

In the following example, a value of 5 is set as the maximum number of archive files of the running configuration to be saved in the Cisco configuration archive:

configure terminal
!
archive
path disk0:myconfig
maximum 5
end

Command	Description
archive config	Saves a copy of the current running configuration to the Cisco configuration archive.
configure confirm	Confirms replacement of the current running configuration with a saved Cisco configuration file.
configure replace	Replaces the current running configuration with a saved Cisco configuration file.
path	Specifies the location and filename prefix for the files in the Cisco configuration archive.
show archive	Displays information about the files saved in the Cisco configuration archive.
time-period	Sets the time increment for automatically saving an archive file of the current running configuration in the Cisco configuration archive.

# memory cache error-recovery

To trace error recovery in memory using caches, use the **memory cache error-recovery** command in global configuration mode. To disable the memory cache error recovery mechanisms, use the **no** form of this command.

memory cache error-recovery {L1| L2| L3} {data| inst}

no memory cache error-recovery {L1| L2| L3} {data| inst}

Syntax Description	L1	Specifies the L1 cache.
	L2	Specifies the L2 cache.
	L3	Specifies the L3 cache.
	data	Specifies if data recovery is required.
	inst	Specifies if instruction recovery is required.

**Command Default** Memory cache error recovery mechanisms are not enabled.

**Command Modes** Global configuration (config)

<b>Command History</b>	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)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.

**Examples** 

I

The following example shows how to enable the **memory cache error-recovery** command:

Router> enable Router# configure terminal Router(config)# memory cache error-recovery

nands	Command	Description
	memory cache error-recovery options	Traces error recovery in memory using caches through
		set options.

٦

# memory cache error-recovery options

To trace error recovery in memory using caches through set options, use the **memory cache error-recovery options**command in global configuration mode. To disable the set memory cache error recovery mechanisms, use the **no** form of this command.

memory cache error-recovery options {abort-if-same-content| blocking-mode| max-recoveries value| nvram-report| parity-check| window seconds}

no memory cache error-recovery options {abort-if-same-content| blocking-mode| max-recoveries value| nvram-report| parity-check| window seconds}

#### **Syntax Description**

abort-if-same-content	Abort recovery if the cache contains the same content as the memory.
blocking-mode	Sets the memory blocking mode to special or ON.
max-recoveries value	The maximum number of recoveries allowed within a time window. Specify a value in the range 0 to 255.
nvram-report	Saves the report in the NVRAM.
parity-check	Sets the parity checking mode to normal or ON.
window seconds	The time window, in seconds. Specify a value in the range 1 to 31536000.

**Command Default** Memory cache error recovery mechanisms are not enabled.

**Command Modes** Global configuration (config)

<b>Command History</b>	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)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.

#### **Examples**

The following example shows how to enable the **memory cache error-recovery options**command:

Router> enable

1

Router# configure terminal Router(config)# memory cache error-recovery options abort-if-same-content

Command	Description
memory cache error-recovery	Traces error recovery in memory using caches.

# memory free low-watermark

To configure a router to issue system logging message notifications when available memory falls below a specified threshold, use the **memory free low-watermark** command in global configuration mode. To disable memory threshold notifications, use the **no** form of this command.

memory free low-watermark {processor threshold| io threshold}

no memory free low-watermark

Syntax Description	processor threshold	Sets the processor memory threshold in kilobytes. When available processor memory falls below this threshold, a notification message is triggered. Valid values are 1 to 4294967295.
	io threshold	Sets the input/output (I/O) memory threshold in kilobytes. When available I/O memory falls below this threshold, a notification message is triggered. Valid values are 1 to 4294967295.

### **Command Default** Memory threshold notifications are disabled.

**Command Modes** Global configuration

<b>Command History</b>	Release	Modification
	12.2(18)S	This command was introduced.
	12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

#### **Usage Guidelines**

I

Using this command, you can configure a router to issue a system logging message each time available free memory falls below a specified threshold ("low-watermark"). Once available free memory rises to 5 percent above the threshold, another notification message is generated.

#### Examples

The following example specifies a free processor memory notification threshold of 20000 KB:

Router (config) # memory free low-watermark processor 200000 If available free processor memory falls below this threshold, the router sends a notification message like this one:

000029: \*Aug 12 22:31:19.559: %SYS-4-FREEMEMLOW: Free Memory has dropped below 20000k Pool: Processor Free: 66814056 freemem\_lwm: 204800000 Once available free processor memory rises to a point 5 percent above the threshold, another notification message like this is sent:

000032: \*Aug 12 22:33:29.411: %SYS-5-FREEMEMRECOVER: Free Memory has recovered 20000k Pool: Processor Free: 66813960 freemem\_lwm: 0

Command	Description	
memory reserve critical	Reserves memory for use by critical processes.	

# memory lite

To enable the memory allocation lite (malloc lite) feature, use the **memory lite** command in global configuration mode. To disable this feature, use the **no** form of this command. memory lite no memory lite **Syntax Description** This command has no arguments or keywords. **Command Default** This command is enabled by default. **Command Modes** Global configuration **Command History** Modification Release 12.3(11)T This command was introduced. **Usage Guidelines** The malloc lite feature was implemented to avoid excessive memory allocation overhead for situations where less than 128 bytes were required. This feature is supported for processor memory pools only. The malloc lite feature is enabled by default. If the malloc lite feature is disabled using the **no memory** litecommand, you can re-enable the feature by entering the memory lite command. **Examples** The following example shows how to disable the malloc\_lite feature: no memory lite **Related Commands** Command Description scheduler heapcheck process Performs a "sanity check" for corruption in memory

blocks when a process switch occurs.

## memory reserve

To reserve a specified amount of memory in kilobytes for console access and critical notifications, use the **memory reserve** command in global configuration mode. To disable the configuration, use the **no** form of this command.

#### Syntax for Releases 15.0(1)M and 12.2(33)SRC and Later Releases

**memory reserve** {**console** *size*| **critical** [ *total-size* ]}

no memory reserve {console| critical}

### Syntax for Releases 12.2(33)SXI, Cisco IOS XE Release 2.1 and Later Releases

memory reserve critical [ total-size ]

no memory reserve critical

#### **Syntax Description**

1	console	Reserves the memory size for a console session.
	size	Amount of memory to be reserved, in kilobytes. The range is from 1 to 4096.
	critical	Reserves the memory for critical notifications.
	total-size	(Optional) Total amount of memory to be reserved, in kilobytes. The range is from 1 to 4294967295.

## **Command Modes** Global configuration (config)

**Command Default** 256 KB is reserved for console memory access. 100 KB is reserved for cricial memory access.

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)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
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.
	15.0(1)M 12.2(33)SRC 12.2(33)SXI

ſ

Usage Guidelines	The <b>memory reserve console</b> command reserves enough memory to ensure console access to a Cisco IOS device for administrative and troubleshooting purposes. This feature is especially beneficial when the device runs low on memory.	
	The <b>memory reserve critical</b> command reserves the specified amount of memory in kilobytes so that the router can issue critical notifications. The amount of memory reserved for critical notifications cannot exceed 25 percent of the total available memory.	
Examples	The following example shows how to reserve a specified amount of memory in kilobytes for console access:	
	Router# <b>configure terminal</b> Router(config)# <b>memory reserve console 2</b>	
<b>Related Commands</b>	Command	Description
	memory free low-watermark	Configures a router to issue system logging message notifications when available memory falls below a specified threshold.

# memory reserve critical

Note

Effective with Cisco IOS Release 12.4(15)T1, the **memory reserve critical** command is replaced by the **memory reserve** command. See the **memory reserve** command for more information.

To configure the size of the memory region to be used for critical notifications (system logging messages), use the **memory reserve critical**command in global configuration mode. To disable the reservation of memory for critical notifications, use the **no** form of this command.

memory reserve critical kilobytes

no memory reserve critical

Syntax Description		Specifies the amount of memory to be reserved in kilobytes. Valid values are 1 to 4294967295, but the value you specify cannot exceed 25 percent of total memory. The default is 100 kilobytes.
--------------------	--	---

**Command Default** 100 kilobytes of memory is reserved for the logging process.

**Command Modes** Global configuration (config)

<b>Command History</b>	Release	Modification
	12.2(18)S	This command was introduced.
	12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.4(15)T1	This command was replaced by the <b>memory reserve</b> command.

#### **Usage Guidelines**

This command reserves a region of memory on the router so that, when system resources are overloaded, the router retains enough memory to issue critical system logging messages.

Γ

<b>Note</b> Once the size of the reserved memory region is specified, only after the current configuration is saved and the syste		on is specified, any change to the specified value takes effect and the system has been reloaded.
Examples	The following example shows how to resersystem restart:	ve 1,000 KB of system memory for logging messages at the next
	Router(config)# memory reserve critic	cal 1000
<b>Related Commands</b>	Command	Description
	memory free low-watermark	Configures a router to issue syslog notifications when available memory falls below a specified threshold.

# memory sanity

To perform a "sanity check" for corruption in buffers and queues, use the **memory sanity** command in global configuration mode. To disable this feature, use the **no** form of this command.

memory sanity [buffer| queue| all]

no memory sanity

Syntax Description	buffer		(Optional) Specifies checking all buffers.
	queue		(Optional) Specifies checking all queues.
	all		(Optional) Specifies checking all buffers and queues.
Command Default	This command is not enable be performed on all buffers		r or <b>queue</b> keyword is not specified, a sanity check will
Command Modes	Global configuration		
Command History	Release	Modifica	ition
	12.2(15)T	This com	nmand was introduced.
Usage Guidelines	<i>i i</i>	a packet buffer is returned	d, a sanity check is performed on buffers when a packet to the buffer pool. This command also time-stamps the a buffer.
The <b>memory sanity</b> command can be saved in the startup configuration file and, therefore, to reconfigure this command each time the router is reloaded. Like the <b>scheduler heapcheck</b> command, the <b>memory sanity</b> command can check for corruption in the I/O memory bloc		oaded. Like the scheduler heapcheck process memory	
	Enabling the <b>memory sani</b>	ty command may result in	slight router performance degradation.
Examples	The following example sho	ows how to perform a sanit	ty check for corruption in all buffers and queues:
	memory sanity all		

## **Related Commands**

ſ

Command	Description
scheduler heapcheck process memory	Performs a "sanity check" for corruption in memory blocks when a process switch occurs.

## memory scan

To enable the Memory Scan feature, use the memory scan command in global configuration mode. To restore the router configuration to the default, use the no form of this command.

memory scan

no memory scan

- **Syntax Description** This command has no arguments or keywords.
- **Command Default** This command is disabled by default.
- **Command Modes** Global configuration

<b>Command History</b>	Release	Modification
	12.0(4)XE	This command was introduced.
	12.0(7)T	This command was integrated in Cisco IOS Release 12.0 T for the Cisco 7500 series only.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

**Usage Guidelines** The Memory Scan feature adds a low-priority background process that searches all installed dynamic random-access memory (DRAM) for possible parity errors. If errors are found in memory areas that are not in use, this feature attempts to scrub (remove) the errors. The time to complete one memory scan and scrub cycle can range from 10 minutes to several hours, depending on the amount of installed memory. The impact of the Memory Scan feature on the central processing unit (CPU) is minimal. To view the status of the memory scan feature on your router, use the **show memory scan** command in EXEC mode.

#### **Examples** The following example enables the Memory Scan feature on a Cisco 7500 series router:

Router(config) # memory scan

Command Descr	ription
show memory scan     Display       system     System	ays the number and type of parity errors on your m.

# memory-size iomem

To reallocate the percentage of DRAM to use for I/O memory and processor memory, use the **memory-size iomem** command in global configuration mode. To revert to the default memory allocation, use the **no** form of this command.

memory-size iomem i/o-memory-percentage

no memory-size iomem

**Syntax Description** 

	i/o-memory-percentage	The percentage of DRAM allocated to I/O memory,	
		in bytes. The values permitted are 5, 10, 15, 20, 25,	
		30, 40, and 50 . A minimum of 4 MB of memory is	
		required for I/O memory.	
L			

**Command Default** 

The default memory allocation is 25 percent of the DRAM to I/O memory and 75 percent of the DRAM to processor memory.

Note

If the **smartinit** process has been enabled, the default memory allocation of 25 percent to the I/O memory does not apply. Instead, **smartinit** examines the network modules, and then calculates the memory allocation for the I/O memory.

**Command Modes** Global configuration (config)

Command HistoryReleaseModification11.2 PThis command was introduced.12.2(33)SRAThis command was integrated into Cisco IOS Release 12.2(33)SRA.12.4(15)T1This command was integrated into Cisco IOS Release 12.4(15)T1.

**Usage Guidelines** When you specify the percentage of I/O memory in the command line, the processor memory automatically acquires the remaining percentage of the DRAM memory.

**Examples** The following example allocates 40 percent of the DRAM memory to I/O memory and the remaining 60 percent to the processor memory:

Router#

1

configure terminal
Router(config)#
memory-size iomem 40
Smart-init will be disabled and new I/O memory size will take effect upon reload.

# menu (EXEC)

I

To display a preconfigured user menu, use the **menu** command in user EXEC or privileged EXEC mode.

menu menu-name

Cuntary Description			
Syntax Description	menu-name		The name of the menu.
Command Modes	User EXEC		
	Privileged EXEC		
Command History	Release	Modification	
	10.0	This command w	was introduced.
	12.2(33)SRA	This command v	was integrated into Cisco IOS Release 12.2(33)SRA.
Usage Guidelines	<ul> <li><b>sage Guidelines</b> A user menu is a type of user interface where text descriptions of actions to be performed are d user. The user can use the menu to select services and functions without having to know the d command-line interface (CLI) commands.</li> <li>Menus can be created for users in global configuration mode, using the commands listed in th Commands" section.</li> </ul>		functions without having to know the details of
			d EXEC level, but if an item in the menu contains a in at the privileged level for the command to succeed.
Examples	The following example invok	es a menu named OnRa	mp:
	Router> menu OnRamp Welcome to OnRamp I Type a number to s Type 9 to exi Read email UNIX Internet acces Resume UNIX connect Resume next connect Exit menu system	select an option; It the menu. Ss	
<b>Related Commands</b>	Command		Description
	menu clear-screen		Clears the terminal screen before displaying a menu.

٦

Command	Description
menu command	Specifies underlying commands for user interface menus.
menu default	Specifies the menu item to use as the default.
menu line-mode	Requires the user to press Enter after specifying an option number.
menu options	Sets options for items in user interface menus.
menu prompt	Specifies the prompt for a user interface menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu status-line	Displays a line of status information about the current user at the top of a menu.
menu text	Specifies the text of a menu item in a user interface menu.
menu title	Creates a title, or banner, for a user menu.
no menu	Deletes a specified menu from a menu configuration.

I

# menu menu-name single-space

To display menu items single-spaced rather than double-spaced, use the **menu <menu-name> single-space** command in global configuration mode.

menu menu-name single-space

Syntax Description	menu-name		Name of the menu this command should be applied to.
Command Default	Enabled for menus with more than	nine items <sup>.</sup> disable	d for menus with nine or fewer items.
		,	
Command Modes	Global configuration		
Command History	Release	Modification	
	10.0	This command was introduced.	
	12.2(33)SRA	This command v	was integrated into Cisco IOS Release 12.2(33)SRA.
Usage Guidelines Examples	with nine or fewer items to display	single-spaced, use	nu is displayed single-spaced. To configure the menus this command. re displayed for the menu named Access1:
Related Commands	Command		Description
	menu (EXEC)		Invokes a user menu.
	menu clear-screen		Clears the terminal screen before displaying a menu.
	menu command		Specifies underlying commands for user menus.
	menu default		Specifies the menu item to use as the default.
	menu line-mode		Requires the user to press Enter after specifying an item.

٦

Command	Description
menu options	Sets options for items in user menus.
menu prompt	Specifies the prompt for a user menu.
menu status-line	Displays a line of status information about the current user at the top of a menu.
menu text	Specifies the text of a menu item in a user menu.
menu title	Creates a title, or banner, for a user menu.

I

# menu clear-screen

To clear the terminal screen before displaying a menu, use the **menu clear-screen** command in global configuration mode.

#### menu clear-screen menu-name clear-screen

Syntax Description	menu-name		Name of the menu this command should be applied to.
Command Default	Disabled		
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	the configured terminal typ of terminals instead of have	be for the user. This comma ing terminal-specific string	m based on termcap entries defined in the router and and allows the same menu to be used on multiple types s embedded within menu titles. If the termcap entry s 24 new lines, causing all existing text to scroll off the
Examples	In the following example, t	the terminal screen is cleared	ed before displaying the menu named Access1:
	Router(config)# <b>menu A</b> d	ccess1 clear-screen	
<b>Related Commands</b>	Command		Description
	menu (EXEC)		Invokes a user menu.
	menu command		Specifies underlying commands for user menus.
	menu default		Specifies the menu item to use as the default.
			1

٦

Command	Description
menu line-mode	Requires the user to press Enter after specifying an item.
menu options	Sets options for items in user menus.
menu prompt	Specifies the prompt for a user menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu status-line	Displays a line of status information about the current user at the top of a menu
menu text	Specifies the text of a menu item in a user menu.
menu title	Creates a title, or banner, for a user menu.
no menu	Deletes a specified menu from a menu configuration.

# menu command

To specify underlying commands for user menus, use the **menu command** command in global configuration mode.

menu command menu menu-name command menu-item {command | menu-exit}

#### **Syntax Description**

menu-name	Name of the menu. You can specify a maximum of 20 characters.
menu-item	Number, character, or string used as the key for the item. The key is displayed to the left of the menu item text. You can specify a maximum of 18 menu entries. When the tenth item is added to the menu, the line-mode and single-space options are activated automatically.
command	Command to issue when the user selects an item.
menu-exit	Provides a way for menu users to return to a higher-level menu or exit the menu system.

#### **Command Default** Disabled

## **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**

I

**es** Use this command to assign actions to items in a menu. Use the **menu text** global configuration command to assign text to items. These commands must use the same menu name and menu selection key.

The **menu command** command has a special keyword for the *command* argument, **menu-exit**, that is available only within menus. It is used to exit a submenu and return to the previous menu level, or to exit the menu altogether and return to the EXEC command prompt.

You can create submenus that are opened by selecting entries in another menu. Use the **menu** EXEC command as the *command* for the submenu item.



If you nest too many levels of menus, the system prints an error message on the terminal and returns to the previous menu level.

When a menu allows connections (their normal use), the command for an entry activating the connection should contain a **resume** command, or the line should be configured to prevent users from escaping their sessions with the **escape-char none** command. Otherwise, when they escape from a connection and return to the menu, there will be no way to resume the session and it will sit idle until the user logs out.

Specifying the **resume** command as the action that is performed for a selected menu entry permits a user to resume a named connection or connect using the specified name, if there is no active connection by that name. As an option, you can also supply the connect string needed to connect initially. When you do not supply this connect string, the command uses the specified connection name.

You can also use the **resume/next** command, which resumes the next connection in the user's list of connections. This function allows you to create a single menu entry that steps through all of the user's connections.

Note

A menu should not contain any exit paths that leave users in an unfamiliar interface environment.

When a particular line should always display a menu, that line can be configured with an **autocommand** line configuration command. Menus can be run on a per-user basis by defining a similar **autocommand** command for that local username. For more information about the **autocommand** command, refer to the *Cisco IOS Dial Technologies Configuration Guide*.

Examples

In the following example, the commands to be issued when the menu user selects option 1, 2, or 3 are specified for the menu named Access1:

menu Access1 command 1 tn3270 vms.cisco.com menu Access1 command 2 rlogin unix.cisco.com menu Access1 command 3 menu-exit The following avanual allows a menu user to avit a menu

The following example allows a menu user to exit a menu by entering Exit at the menu prompt:

menu Access1 text Exit Exit menu Access1 command Exit menu-exit

Command	Description
autocommand	Configures the Cisco IOS software to automatically execute a command when a user connects to a particular line.
menu (EXEC)	Invokes a user menu.
menu clear-screen	Clears the terminal screen before displaying a menu.
menu default	Specifies the menu item to use as the default.
menu line-mode	Requires the user to press Enter after specifying an item.

Command	Description
menu options	Sets options for items in user menus.
menu prompt	Specifies the prompt for a user menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu status-line	Displays a line of status information about the current user at the top of a menu
menu text	Specifies the text of a menu item in a user menu.
menu title	Creates a title, or banner, for a user menu.

# menu default

To specify the menu item to use as the default, use the **menu default** command in global configuration mode.

menu menu-name default menu-item

Syntax Description	menu-name	Name of the menu. You can specify a maximum of 20 characters.
	menu-item	Number, character, or string key of the item to use as the default.
Command Default	Disabled	
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		which menu entry is used when the user presses Enter without specifying an efined by the <b>menu command</b> and <b>menu text</b> global configuration commands.
Examples	In the following example, th	e menu user exits the menu when pressing Enter without selecting an item:
	menu Accessl 9 text Exit menu Accessl 9 command r menu Accessl default 9	
<b>Related Commands</b>	Command	Description
	menu (EXEC)	Invokes a preconfigured user menu.
	menu command	Specifies underlying commands for user menus.

Specifies the prompt for a user menu.

1

menu prompt

I

Command	Description
menu text	Specifies the text of a menu item in a user menu.
menu title	Creates a title, or banner, for a user menu.

# menu line-mode

To require the user to press Enter after specifying an item, use the **menu line-mode** command in global configuration mode.

menu menu-name line-mode

Syntax Description	menu-name		Name of the menu this command should be applied to.
Command Default	Enabled for menus with me	ore than nine items. Disabl	ed for menus with nine or fewer items.
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	you select a menu entry by over the selected number a This option is activated aut explicitly for menus of nin	entering the item number a nd enter another number be omatically when more than e or fewer items.	a menu item by entering the item number. In line mode, and pressing Enter. Line mode allows you to backspace efore pressing Enter to issue the command. nine menu items are defined but also can be configured <b>e-mode</b> command must be configured.
Examples	In the following example, menu Access1 line-mode	the line-mode option is ena	bled for the menu named Access1:
<b>Related Commands</b>	Command		Description
	menu (EXEC)		Invokes a preconfigured user menu.
	menu clear-screen		Clears the terminal screen before displaying a menu.
	menu command		Specifies underlying commands for a user menu.

Command	Description
menu default	Specifies the menu item to use as the default.
menu options	Sets options for items in user menus.
menu prompt	Specifies the prompt for a user menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu status-line	Displays a line of status information about the current user at the top of a menu.
menu text	Specifies the text of a menu item in a user menu.

## menu options

To set options for items in user menus, use the **menu options** command in global configuration mode.

#### Cisco IOS Release 10.0, 12.2(33)SRA, 12.2(33)SXI , and Later Releases

menu menu-name options menu-item [login] [pause]

#### **Cisco IOS XE Release 3.1S and Later Releases**

menu menu-name options menu-item {login| pause}

#### **Syntax Description**

menu-name	The name of the menu. You can specify a maximum of 20 characters.
menu-item	Number, character, or string key of the item affected by the option.
login	(Optional) Configures the router to request a login before issuing the command.
pause	(Optional) Configures the router to pause after issuing the command and before redrawing the menu.

#### **Command Default** The menu options are disabled.

#### **Command Modes** Global configuration (config)

# Command HistoryReleaseModification10.0This command was introduced.12.2(33)SRAThis command was integrated into Cisco IOS Release 12.2(33)SRA.12.2(33)SXIThis command was integrated into a release earlier than Cisco IOS<br/>Release 12.2(33)SXI.Cisco IOS XE Release 3.1SThis command was integrated into a release earlier than Cisco IOS<br/>Release 3.1S.

#### **Usage Guidelines**

Use the **menu command** and **menu text** commands to define a menu entry.

**Examples** 

I

The following example shows how to configure the router to request a login before issuing the command specified by menu entry 3 of the menu named Access1:

Router(config)# menu Access1 options 3 login

#### **Related Commands**

Command	Description
menu (EXEC)	Invokes a user menu.
menu clear-screen	Clears the terminal screen before displaying a menu.
menu command	Specifies underlying commands for user menus.
menu default	Specifies the menu item to use as the default.
menu line-mode	Requires the user to press Enter after specifying an item.
menu prompt	Specifies the prompt for a user menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu status-line	Displays a line of status information about the current user at the top of a menu.
menu text	Specifies the text of a menu item in a user menu.
menu title	Creates a title, or banner, for a user menu.

# menu prompt

To specify the prompt for a user menu, use the **menu prompt** command in global configuration mode.

menu menu-name prompt d prompt d

Syntax Description	menu-name	Name of the menu. You can specify a maximum of 20 characters.
	d	A delimiting character that marks the beginning and end of a title. Text delimiters are characters that do not ordinarily appear within the text of a title, such as slash ( / ), double quote ("), and tilde (~). ^C is reserved for special use and should not be used in the text of the title.
	prompt	Prompt string for the menu.
Command Default	Disabled	
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	text followed by the delimi	he first delimiter. The router will prompt you for the text of the prompt. Enter the ter, and press Enter. nd <b>menu text</b> commands to define the menu selections.
	ose die menu communu d	
Examples	In the following example, the prompt for the menu named Access1 is configured as "Select	
	Router(config) <b># menu Ac</b> Enter TEXT message. Er <b>Select an item. /</b>	ccess1 prompt / nd with the character '/'.

#### **Related Commands**

ſ

Command	Description
menu (EXEC)	Invokes a user menu.
menu command	Specifies underlying commands for user menus.
menu default	Specifies the menu item to use as the default.
menu text	Specifies the text of a menu item in a user menu.
menu title	Creates a title, or banner, for a user menu.

# menu status-line

To display a line of status information about the current user at the top of a menu, use the **menu status-line** command in global configuration mode.

menu menu-name status-line

Syntax Description	menu-name		Name of the menu this command should be applied
			to.
Command Default	Disabled		
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	1.		op of the screen before the menu title is displayed. This ine number, and the current terminal type and keymap
Examples	In the following example, s	tatus information is enable	ed for the menu named Access1:
	menu Access1 status-lin	e	
<b>Related Commands</b>	Command		Description
	menu (EXEC)		Invokes a user menu.
	menu clear-screen		Clears the terminal screen before displaying a menu.
	menu command		Specifies underlying commands for user menus.

Specifies the menu item to use as the default.

1

menu default

Command	Description
menu line-mode	Requires the user to press Enter after specifying an item in a menu.
menu options	Sets options for items in user menus.
menu prompt	Specifies the prompt for a user menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu text	Specifies the text of a menu item in a user menu.
menu title	Creates a title, or banner, for a user menu.

### menu text

To specify the text of a menu item in a user menu, use the menu text command in global configuration mode.

menu menu-name text menu-item menu-text

#### **Syntax Description**

menu-name	Name of the menu. You can specify a maximum of 20 characters.
menu-item	Number, character, or string used as the key for the item. The key is displayed to the left of the menu item text. You can specify a maximum of 18 menu items. When the tenth item is added to the menu, the <b>menu line-mode</b> and <b>menu single-space</b> commands are activated automatically.
menu-text	Text of the menu item.

#### **Command Default** No text appears for the menu item.

#### **Command Modes** Global configuration

<b>Command History</b>	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 assign text to items in a menu. Use the **menu command** command to assign actions to items. These commands must use the same menu name and menu selection key.

You can specify a maximum of 18 items in a menu.

#### **Examples**

In the following example, the descriptive text for the three entries is specified for options 1, 2, and 3 in the menu named Access1:

```
menu Access1 text 1 IBM Information Systems
menu Access1 text 2 UNIX Internet Access
menu Access1 text 3 Exit menu system
```

#### **Related Commands**

ſ

Command	Description
menu (EXEC)	Invokes a user menu.
menu clear-screen	Clears the terminal screen before displaying a menu.
menu command	Specifies underlying commands for user menus.
menu default	Specifies the menu item to use as the default.
menu line-mode	Requires the user to press Enter after specifying an item.
menu options	Sets options for items in user menus.
menu prompt	Specifies the prompt for a user menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu status-line	Displays a line of status information about the current user at the top of a menu.
menu title	Creates a title, or banner, for a user menu.

# menu title

To create a title (banner) for a user menu, use the **menu title** command in global configuration mode.

menu menu-name title d menu-title d

#### **Syntax Description**

menu-name	Name of the menu. You can specify a maximum of 20 characters.
d	A delimiting character that marks the beginning and end of a title. Text delimiters are characters that do not ordinarily appear within the text of a title, such as slash ( $/$ ), double quote ("), and tilde ( $\sim$ ). $^{C}$ is reserved for special use and should not be used in the text of the title.
menu-title	Lines of text to appear at the top of the menu.

#### **Command Default** The menu does not have a title.

#### **Command Modes** Global configuration

<b>Command History</b>	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 **menu title** command must use the same menu name used with the **menu text** and **menu command** commands used to create a menu.

You can position the title of the menu horizontally by preceding the title text with blank characters. You can also add lines of space above and below the title by pressing Enter.

Follow the **title** keyword with one or more blank characters and a delimiting character of your choice. Then enter one or more lines of text, ending the title with the same delimiting character. You cannot use the delimiting character within the text of the message.

When you are configuring from a terminal and are attempting to include special control characters, such as a screen-clearing string, you must use Ctrl-V before the special control characters so that they are accepted as part of the title string. The string ^[[H^[]J is an escape string used by many VT100-compatible terminals to clear the screen. To use a special string, you must enter Ctrl-V before each escape character.

You also can use the **menu clear-screen** global configuration command to clear the screen before displaying menus and submenus, instead of embedding a terminal-specific string in the menu title. The **menu clear-screen** command allows the same menu to be used on different types of terminals.

```
Examples
```

In the following example, the title that will be displayed is specified when the menu named Access1 is invoked. Press Enter after the second slash (/) to display the prompt.

```
Router(config) # menu Access1 title /^[[H^[[J
Enter TEXT message. End with the character '/'.
Welcome to Access1 Internet Services
```

Type a number to select an option; Type 9 to exit the menu.

, Router(config)#

#### **Related Commands**

Command	Description
menu (EXEC)	Invokes a user menu.
menu clear-screen	Clears the terminal screen before displaying a menu.
menu command	Specifies underlying commands for user menus.
menu default	Specifies the menu item to use as the default.
menu line-mode	Requires the user to press Enter after specifying an item.
menu options	Sets options for items in user menus.
menu prompt	Specifies the prompt for a user menu.
menu single-space	Displays menu items single-spaced rather than double-spaced.
menu status-line	Displays a line of status information about the current user at the top of a menu.
menu text	Specifies the text of a menu item in a user menu.

# microcode (12000)

To load a Cisco IOS software image on a line card from Flash memory or the GRP card on a Cisco 12000 series Gigabit Switch Router (GSR), use the **microcode** command in global configuration mode. To load the microcode bundled with the GRP system image, use the **no** form of this command.

microcode {oc12-atm| oc12-pos| oc3-pos4} {flash *file-id* [ *slot* ]| system [ *slot* ]} no microcode {oc12-atm| oc12-pos| oc3-pos4} [flash *file-id* [ *slot* ]| system [ *slot* ]]

#### **Syntax Description**

oc12-atm   oc12-pos   oc3-pos4	Interface name.
flash	Loads the image from the Flash file system.
file-id	<ul> <li>Specifies the device and filename of the image file to download from Flash memory. A colon (:) must separate the device and filename (for example, slot0:gsr-p-mz). Valid devices include:</li> <li>bootflash:Internal Flash memory.</li> <li>slot0:First PCMCIA slot.</li> <li>slot1:Second PCMCIA slot.</li> </ul>
slot	(Optional) Slot number of the line card that you want to copy the software image to. Slot numbers range from 0 to 11 for the Cisco 12012 router and 0 to 7 for the Cisco 12008 router. If you do not specify a slot number, the Cisco IOS software image is downloaded on all line cards.
system	Loads the image from the software image on the GRP card.

**Command Default** The default is to load the image from the GRP card (system).

**Command Modes** Global configuration

#### **Command Histor**

nd History	Release	Modification
	11.2 GS	This command was introduced for Cisco 12000 series GSRs.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

ſ

Usage Guidelines	In addition to the Cisco IOS image that resides on the GRP card, each line card on a Cisco 12000 series has a Cisco IOS image. When the router is reloaded, the specified image is loaded onto the GRP card and ther automatically downloaded to all the line cards.		
	Normally, you want the same Cisco IOS image on the GRP card and all line cards. However, i upgrade a line card with a new version of microcode for testing or to fix a defect, you might n Cisco IOS image that is different from the one on the line card. Additionally, you might need to mage on the line card to work around a problem that is affecting only one of the line cards.		
	To load a Cisco IOS image on a line card, first use the <b>copy tftp</b> command to download the Cisco IOS image to a slot on one of the PCMCIA Flash memory cards. Then use the <b>microcode</b> command to download the image to the line card, followed by the <b>microcode reload</b> command to start the image. Immediately after you enter the <b>microcode reload</b> command and press Return, the system reloads all microcode. Global configuration mode remains enabled. After the reloading is complete, enter the <b>exit</b> command to return to the EXEC system prompt.		
	To verify that the correct image is running on the line ca	rd, use the <b>execute-on slot</b> <i>slot</i> <b>show version</b> command.	
	For additional information on GSR configuration, refe software release.	er to the documentation specific to your Cisco IOS	
Examples	In the following example, the Cisco IOS software image in slot 0 is downloaded to the line card in slot 10. This software image is used when the system is booted, a line card is inserted or removed, or the <b>microcode reload</b> global configuration command is issued.		
	Router(config)# microcode oc3-POS-4 flash slot0:fip.v141-7 10 Router(config)# microcode reload 10 In this example, the user would issue the execute-on slot 10 show version command to verify that the correct version is loaded.		
<b>Related Commands</b>	Command	Description	
	Command	Description	
	microcode reload (12000)	Reloads microcode on Cisco 12000 series GSRs.	

# microcode (7000/7500)

To specify the location of the microcode that you want to download from Flash memory into the writable control store (WCS) on Cisco 7000 series (including RSP based routers) or Cisco 7500 series routers, use the **microcode** command in global configuration mode. To load the microcode bundled with the system image, use the **no** form of this command.

**microcode** *interface-type* {*flash-filesystem:filename* [ *slot* ]| **rom**| **system** [ *slot* ]} **no microcode** *interface-type* {*flash-filesystem:filename* [ *slot* ]| **rom**| **system** [ *slot* ]}

#### **Syntax Description**

interface-type	One of the following interface processor names: <b>aip</b> , <b>cip</b> , <b>eip</b> , <b>feip</b> , <b>fip</b> , <b>fsip</b> , <b>hip</b> , <b>mip</b> , <b>sip</b> , <b>sp</b> , <b>ssp</b> , <b>trip</b> , <b>vip</b> , or <b>vip2</b>
flash-filesystem :	Flash file system, followed by a colon . Valid file systems are <b>bootflash</b> , <b>slot0</b> , and <b>slot1</b>
	Slave devices such as slaveslot0 are invalid. The slave's file system is not available during microcode reloads.
filename	Name of the microcode file.
slot	(Optional) Number of the slot. Range is from 0 to 15.
rom	If ROM is specified, the router loads from the onboard ROM microcode.
system	If the <b>system</b> keyword is specified, the router loads the microcode from the microcode bundled into the system image you are running for that interface type.

**Command Default** The default is to load from the microcode bundled in the system image.

**Command Modes** Global configuration

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

Comm

ſ

Usage Guidelines	If you do not use the <b>microcode reload</b> command after using the <b>microcode</b> command, the <b>microcode reload</b> command will be written to the configuration file automatically.		
	same microcode image in the same location when the	ensure that the master and slave RSP card contain the router is to load the interface processor microcode from he master, it will be able to find the microcode image	
Examples	In the following example, all FIP cards will be loaded with the microcode found in Flash memoryfile fip.v141-7 when the system is booted, when a card is inserted or removed, or when the <b>microcode reload</b> global configuration command is issued. The configuration is then written to the startup configuration file.		
	Router(config)# microcode fip slot0:fip.v141-7 Router(config)# end Router# copy system:running-config nvram:startup-config		
<b>Related Commands</b>	s Command Description		
	more flh:logfile	Displays the system console output generated during the Flash load helper operation.	

# microcode (7200)

To configure a default override for the microcode that is downloaded to the hardware on a Cisco 7200 series router, use the **microcode** command in global configuration mode. To revert to the default microcode for the current running version of the Cisco IOS software, use the **no** form of this command.

microcode {ecpa| pcpa} location

no microcode {ecpa| pcpa}

#### **Syntax Description**

есра	ESCON Channel Port Adapter (CPA) interface.
рсра	Parallel CPA interface.
location	Location of microcode, including the device and filename.

# **Command Default** If the default or **no**form of the command is specified, the driver uses the default microcode for the current running version of the Cisco IOS software.

#### **Command Modes** Global configuration

Command History	Release	Modification
	11.3(3)T	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

#### **Usage Guidelines**

idelines If there are any default overrides when the configuration is written, then the **microcode reload** command will be written to the configuration automatically. This action enables the configured microcode to be downloaded at system startup.

The CPA microcode image is preloaded on Flash memory cards for Cisco 7200-series routers for Cisco IOS Release 11.3(3)T and later releases. You may be required to copy a new image to Flash memory when a new microcode image becomes available.

For more information on the CPA configuration and maintenance, refer to the "Configuring Cisco Mainframe Channel Connection Adapters" chapter in the *Release 12.2 Cisco IOS Bridging and IBM Networking Configuration Guide.* 

**Examples** The following example instructs the Cisco IOS software to load the microcode from an individual microcode image that is stored as a file on the Flash card inserted in Flash card slot 0:

microcode ecpa slot0:xcpa26-1

#### **Related Commands**

Command	Description
microcode reload (7200)	Resets and reloads the specified hardware in a Cisco 7200 series router.
show microcode	Displays microcode information.

# microcode reload (12000)

To reload the Cisco IOS image from a line card on Cisco 12000 series routers, use the **microcode reload** command in global configuration mode.

microcode reload [ slot-number ]

**Syntax Description** 

slot-number	(Optional) Slot number of the line card that you want to reload the Cisco IOS software image on. Slot numbers range from 0 to 11 for the Cisco 12012 and from 0 to 7 for the Cisco 12008 router. If you do not specify a slot number, the Cisco IOS software image is reloaded on all line cards.
-------------	--

#### **Command Modes** Global configuration

Release	Modification
11.2 GS	This command was introduced for Cisco 12000 series GSRs.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

# **Usage Guidelines** In addition to the Cisco IOS image that resides on the GRP card, each line card on Cisco 12000 series routers has a Cisco IOS image. When the router is reloaded, the specified Cisco IOS image is loaded onto the GRP card and automatically downloaded to all the line cards.

Normally, you want the same Cisco IOS image on the GRP card and all line cards. However, if you want to upgrade a line card with a new version of microcode for testing or to fix a defect, you might need to load a different Cisco IOS image. Additionally, you might need to load a new image on the line card to work around a problem affecting only one of the line cards.

To load a Cisco IOS image on a line card, first use the **copy tftp** command to download the Cisco IOS image to a slot on one of the PCMCIA Flash memory cards. Then use the **microcode** command to download the image to the line card, followed by the **microcode reload** command to start the image. To verify that the correct image is running on the line card, use the **execute-on slot** *slot* **show version** command.

For additional information on GSR configuration, refer to the "Observing System Startup and Performing a Basic Configuration" chapter in the Cisco 12000 series installation and configuration guides.

The microcode reload (12000) command allows you to issue another command immediately.

Ø
Note

Issuing a **microcode reload** command on any of the line cards in a Cisco 12000 GSR immediately returns the console command prompt. This allows you to issue a subsequent command immediately to the reloading line card. However, any commands entered at this time will not execute, and often no indication will be given that such a command failed to run. Verify that the microcode has reloaded before issuing new commands.

#### **Examples**

In the following example, the mirocode firmware is reloaded on the line card in slot 10:

Router(config) # microcode reload 10

#### **Related Commands**

Command	Description
microcode (12000)	Loads a Cisco IOS software image on a line card from Flash memory or the GRP card on a Cisco 12000 series GSR.

# microcode reload (7000 7500)

To reload the processor card on the Cisco 7000 series with RSP7000 or Cisco 7500 series routers, use the **microcode reload** command in global configuration mode.

microcode reload [ slot-number ]

Syntax Description	slot-number	(Optional) Reloads the specified processor card on a Cisco 7500 series router.
- ,	slot-number	

**Command Default** No default behaviors or values.

**Command Modes** Global configuration

Release	Modification
10.3	This command was introduced for Cisco 7500 series routers.
12.3(8)T	The <i>slot-number</i> argument was added for Cisco 7500 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA

**Usage Guidelines** 

**Command H** 

This command reloads the microcode without rebooting the router. Immediately after you enter the **microcode reload** command, the system reloads all microcode. Global configuration mode remains enabled.

**Note** If you modify the system configuration to load a microcode image, the **microcode reload** command will be written to the configuration file automatically following the use of a **microcode** command. This action enables the configured microcode to be downloaded at system startup.

Examples

In the following example, all controllers are reset, and the microcode specified in the current configuration is loaded:

Router(config) # microcode reload

#### **Related Commands**

ſ

Command	Description
microcode (7000/7500)	Specifies the location from where microcode should be loaded when the <b>microcode reload</b> command is processed on RSP-based routers.

# microcode reload (7200)

To reload the Cisco IOS microcode image on an ESCON CPA card in the Cisco 7200 series router, use the **microcode reload** command in privileged EXEC mode.

microcode reload {all| ecpa [slot *slot-number*]| pcpa [slot *slot-number*]}

Syntax Description	all	Resets and reloads all hardware types that support downloadable microcode.
	есра	Resets and reloads only those slots that contain hardware type <b>ecpa</b> .
	рсра	Resets and reloads only those slots that contain hardware type <b>pcpa</b> .
	slot slot-number	(Optional) Resets and reloads only the slot specified, and only if it contains the hardware specified.

#### **Command Modes** Privileged EXEC

Command History	Release	Modification	
	11.3(3)T	This command was introduced.	
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.	
Usage Guidelines	Hardware types that do not support downloadable microcode are unaffected by the microcode reload all		
	command. You will be prompted for confirmation before the <b>microcode reload</b> command is executed.		
Examples	The following example reloads the ESCON CPA microcode in slot 5 with the currently configured microc		
	Router# microcode reload ecpa slot 5		

#### **Related Commands**

Command	Description
microcode (7200)	Configures a default override for the microcode that is downloaded to the hardware on a Cisco 7200 series router.
show microcode	Displays the microcode bundled into a Cisco 7000 series with RSP7000, Cisco 7200 series, or Cisco 7500 series router.

# mkdir

To create a new directory in a Class C flash file system, use the **mkdir** command in user EXEC, privileged EXEC, or diagnostic mode.

**mkdir** *directory* 

Syntax Description	directory	The name of the directory to create.

**Command Modes** User EXEC (>) Privileged EXEC (#) Diagnostic (diag)

<b>Command History</b>	Release	Modification
	11.3AA	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 modified and implemented on the Cisco ASR 1000 Aggregation Services Routers. The following enhancements were made:
		• This command was introduced in diagnostic mode. The command can be entered in both privileged EXEC and diagnostic mode on the Cisco ASR 1000 Series Routers.
		• The harddisk:, obfl:, stby-harddisk:, stby-nvram:, stby-obfl:, stby-usb[0-1]:,and usb[0-1]: <i>directory</i> options were added.

**Usage Guidelines** This command is valid only on Class C flash file systems.

When executing the **mkdir** *directory* command on a USB token device, you can create only two levels of subdirectories under a directory. A new directory (third level directory) cannot be created on the USB token, but you can copy files to the existing subdirectories.

#### **Examples** The following example creates a directory named newdir:

```
Router# mkdir newdir
Mkdir file name [newdir]?
Created dir flash:newdir
Router# dir
Directory of flash:
2 drwx 0 Mar 13 1993 13:16:21 newdir
8128000 bytes total (8126976 bytes free)
```

#### **Related Commands**

Command	Description
dir	Displays a list of files on a file system.
rmdir	Removes an existing directory in a Class C flash file system.

# mkdir disk0:

To create a new directory in a Flash file system, use the mkdir disk0:command.

mkdir disk0:

- **Syntax Description** This command has no arguments or keywords.
- **Command Default** This command has no default settings.

#### Command Modes 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 the 12.2 SX release.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage GuidelinesThis command is valid only on Flash file systems.After you enter the mkdir disk0: command, you are prompted to enter the new directory filename.To check your entry, enter the dir command.To remove a directory, enter the rmdir command.

#### **Examples** This example shows how to create a directory named newdir:

Router# mkdir disk0: Create directory filename [ ]? newdir Created dir disk0: newdir Router#

#### **Related Commands**

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.
rmdir	Removes an existing directory in a Class C Flash file system.

# mode

To set the redundancy mode, use the mode command in redundancy configuration mode.

#### Syntax for 12.2S Release

mode {rpr| rpr-plus| sso}

#### Syntax for Cisco IOS XE Release 2.5 and Later Releases

mode  $\{rpr|sso\}$ 

#### Syntax for 12.2XNE Release

mode sso

#### **Syntax Description**

rpr	Specifies Route Processor Redundancy (RPR) mode.
rpr-plus	Specifies Route Processor Redundancy Plus (RPR+) mode.
\$\$0	Specifies stateful switchover (SSO) mode.

#### **Command Default**

Command Default	• The default is SSO mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.
	• The default is RPR mode if different versions are installed.
	• If redundancy is enabled, the default is the mode that you have configured.
Command Default	• The default is RPR+ mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.
	• The default is RPR mode if different versions are installed.
	• If redundancy is enabled, the default is the mode that you have configured.
Command Default	<ul> <li>The default is SSO mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.</li> <li>The default is RPR mode if different versions are installed.</li> </ul>

#### **Command Default**

• The default is SSO mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.

• The default is RPR mode if different versions are installed.

**Command Modes** Redundancy configuration (config-red)

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was modified. Support was added for SSO mode and the default mode change.
12.2(17d)SXB	This command was modified. Support was added for multicast and unicast traffic.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)XNE	This command was modified. This command was implemented on the Cisco 10000 router.
Cisco IOS XE Release 2.5	This command was modified. This command was implemented on the Cisco ASR 1000 Series Routers.
	12.2(14)SX       12.2(17b)SXA       12.2(17d)SXB       12.2(33)SRA       12.2(33)XNE

#### Usage Guidelines Cisco IOS Release 12.2S and 7600 Series Routers

SSO is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

On releases prior to Release 12.2(17d)SXB, single router mode (SRM) with SSO redundancy does not support stateful switchover for multicast traffic. When a switchover occurs, all multicast hardware switching entries are removed and are then re-created and reinstalled in the hardware by the newly active multilayer switch feature card (MSFC).

SRM/SSO is supported in the following releases only:

- Release 12.2(17b)SXA and subsequent rebuilds.
- Release 12.2(17d)SXB and subsequent rebuilds.

Nonstop forwarding (NSF) with SSO redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, Internetwork Packet Exchange (IPX), and Multiprotocol Label Switching (MPLS).

If you have configured MPLS on the Cisco 7600 series routers with redundant supervisor engines, you must configure the Cisco 7600 series router in RPR mode. The switch should not be running in the default mode of SSO.

Enter the **redundancy** command in global configuration mode to enter redundancy configuration mode. You can enter the **mode** command within redundancy configuration mode.

Follow these guidelines when configuring your system for RPR+ mode:

- You must install compatible images on the active and standby supervisor engines to support RPR+ mode and SSO mode.
- Both supervisor engines must run the same Cisco IOS software version.
- Any modules that are not online at the time of a switchover are reset and reloaded on a switchover.
- The Forwarding Information Base (FIB) tables are cleared on a switchover. As a result, routed traffic is interrupted until route tables reconverge.

The standby supervisor engine reloads on any change of mode and begins to work in the current mode. When you use this command to force the standby supervisor engine to run as a Distributed Forwarding Card (DFC) card, the uplink ports in the standby engine continue to be in use and are not disabled.

#### Cisco IOS Release XE Release 2.5 and ASR 1000 Series Routers

For Cisco ASR 1002 and 1004 routers, RRP and stateful switchover can be used to switch between Cisco IOS processes. RPR and SSO need to be configured by the user, however, because a second Cisco IOS process is not available by default on Cisco ASR 1002 and 1004 routers. Enter the **redundancy** command in global configuration mode to enter redundancy configuration mode. You can enter the **mode** command within redundancy configuration mode.

The Cisco ASR 1006 Router supports a second Route Processor. The second Cisco IOS process can run only on the standby Route Processor. This means that hardware redundancy is available and RPR and SSO do not need to be configured by the user because a second Cisco IOS process is available by default on the Cisco ASR 1006 router.

RPR+ mode is not supported on the Cisco ASR 1000 Series Routers.

#### **Cisco IOS Release 12.2XNE and 1000 Series Routers**

Enter the **redundancy** command in global configuration mode to enter redundancy configuration mode. You can enter the **mode** command within redundancy configuration mode.

RPR mode is not supported on the Cisco 10000 router.

**Examples** This example shows how to set the redundancy mode to RPR+:

Router (config) # redundancy Router (config-red) # mode rpr-plus This example shows how to set the redundancy mode to SSO:

Router(config)# **redundancy** Router(config-red)# **mode sso** 

#### **Related Commands**

Command	Description
redundancy	Enters redundancy configuration mode.
redundancy force-switchover	Forces a switchover from the active to the standby supervisor engine.

Command	Description
route-converge-interval	Configures the time interval after which the old FIB entries are purged.
show redundancy	Displays RF information.
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

٦