

# event application

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of an event raised through the EEM Event Publish application programming interface (API), use the **event application** command in applet configuration mode. To remove the application event criteria, use the **no** form of this command.

```
event application sub-system sub-system-id type event-type
```

```
no event application sub-system sub-system-id type event-type
```

Syntax Description	sub-system	type
	Specifies an identifier for the subsystem named in the <i>sub-system-id</i> argument that will publish the application event. <ul style="list-style-type: none"> <li><i>sub-system-id</i>—Identifier of the subsystem. Number in the range from 1 to 4294967295. If the event is to be published by an EEM policy, the <i>sub-system-id</i> reserved for a policy is 798.</li> </ul>	Specifies the value of an event type within the specified event. <ul style="list-style-type: none"> <li><i>event-type</i>—Event type value. Number in the range from 1 to 4294967295.</li> </ul>

**Defaults** No EEM event criteria are specified.

**Command Modes** Applet configuration

Command History	Release	Modification
	12.2(25)S	This command was introduced.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

**Usage Guidelines** An EEM event is triggered when an application calls the EEM Event Publish API with an event specification that matches the subsystem ID and application event type.

**Examples** The following example shows how a policy named EventPublish\_A runs every 20 seconds and publishes an event to a well-known EEM event type numbered 1. A second policy named EventPublish\_B is registered to run when the well-known EEM event type of 1 occurs. When policy EventPublish\_B runs, it outputs a message to syslog containing data passed as an argument from EventPublish\_A.

```
Router(config)# event manager applet EventPublish_A
Router(config-applet)# event timer watchdog time 20.0
Router(config-applet)# action 1.0 syslog msg "Applet EventPublish_A"
Router(config-applet)# action 2.0 publish-event sub-system 798 type 1 arg1 twenty
Router(config-applet)# exit
Router(config)# event manager applet EventPublish_B
```

```
Router(config-applet)# event application sub-system 798 type 1
Router(config-applet)# action 1.0 syslog msg "Applet EventPublish_B arg1
$_application_data1"
```

---

**Related Commands**

---

<b>Command</b>	<b>Description</b>
<b>event manager applet</b>	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

---

## event cli

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run by matching a Cisco IOS command-line interface (CLI) command, use the **event cli** command in applet configuration mode. To remove the CLI command event criteria, use the **no** form of this command.

```
event cli pattern regular-expression sync {yes | no {skip {yes | no}}} [occurs num-occurrences] [period period-value]
```

```
no event cli pattern regular-expression sync {yes | no {skip {yes | no}}} [occurs num-occurrences] [period period-value]
```

Syntax Description	
<b>pattern</b>	Specifies the regular expression used to perform the CLI command pattern match. <ul style="list-style-type: none"> <li><i>regular-expression</i>—Regular expression. If the expression contains embedded blanks, enclose it in double quotation marks.</li> </ul>
<b>sync</b>	Indicates whether the policy should be executed. The event detector will be notified when the policy completes running, and the exit status of the policy determines whether the CLI command will be executed. If the policy exit status is zero—the policy ran successfully—the CLI command will not be executed; otherwise the CLI command will run. <ul style="list-style-type: none"> <li>If the <b>yes</b> keyword is specified, the policy will run.</li> <li>If the <b>no</b> keyword is specified, the policy will not run.</li> </ul>
<b>skip</b>	Indicates whether the CLI command should be executed. This keyword is required if the <b>sync</b> keyword is followed by the <b>no</b> keyword. If the <b>sync</b> keyword is followed by the <b>yes</b> keyword, the <b>skip</b> keyword should not be specified. <ul style="list-style-type: none"> <li>If the <b>yes</b> keyword is specified, the CLI command should not be executed.</li> <li>If the <b>no</b> keyword is specified, the CLI command should be executed. This is the default.</li> </ul>
<b>occurs</b>	(Optional) Specifies the number of matching occurrences before an EEM event is triggered. If a number is not specified, an EEM event is triggered after the first match. <ul style="list-style-type: none"> <li><i>num-occurrences</i>—The number of occurrences. The value must be greater than 0.</li> </ul>
<b>period</b>	(Optional) Specifies the time interval during which the one or more occurrences must take place. If the keyword is not specified, no time period check is applied. <ul style="list-style-type: none"> <li><i>period-value</i>—Number that represents seconds and optional milliseconds in the format <i>sssss[.mmm]</i>. The range for seconds is from 0 to 4294967295. The range for milliseconds is from 0 to 999. If using milliseconds only, specify the milliseconds in the format <i>0.mmm</i>.</li> </ul>

### Defaults

No EEM events are triggered on the basis of a match with a Cisco IOS CLI command.

**Command Modes** Applet configuration

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

**Usage Guidelines** Use the **event cli** command to set up event criteria against which CLI commands are matched. CLI commands are compared against a specified regular expression. After a specified number of matches occurs within a specified time period, an EEM event is triggered. If multiple conditions exist, the EEM event is triggered when all the conditions are met.

**Examples** The following example shows how to specify an EEM applet to run when the Cisco IOS **interface loopback** CLI command is configured three times. The applet runs the **no shutdown** command to ensure that the loopback interfaces are operational.

```
Router(config)# event manager applet cli-match
Router(config-applet)# event cli pattern {.*interface loopback*} sync yes occurs 3
Router(config-applet)# action 1.0 cli command "no shutdown"
```

Related Commands	Command	Description
	<b>event manager applet</b>	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

## event counter

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of a named counter crossing a threshold, use the **event counter** command in applet configuration mode. To remove the counter event criteria, use the **no** form of this command.

**event counter name** *counter-name* **entry-op** *operator* **entry-val** *entry-value* [**exit-op** *operator*] [**exit-val** *exit-value*]

**no event counter name** *counter-name* **entry-op** *operator* **entry-val** *entry-value* [**exit-op** *operator*] [**exit-val** *exit-value*]

Syntax Description	
<b>name</b>	Specifies that the counter named in the <i>counter-name</i> argument will be monitored. <ul style="list-style-type: none"> <li><i>counter-name</i>—Name of the counter.</li> </ul>
<b>entry-op</b>	Compares the contents of the current counter value with the entry value using the specified operator. If there is a match, an event is triggered and event monitoring is disabled until the exit criteria are met. The <i>operator</i> argument takes one of the following values: <ul style="list-style-type: none"> <li><b>gt</b>—Greater than.</li> <li><b>ge</b>—Greater than or equal to.</li> <li><b>eq</b>—Equal to.</li> <li><b>ne</b>—Not equal to.</li> <li><b>lt</b>—Less than.</li> <li><b>le</b>—Less than or equal to.</li> </ul>
<b>entry-val</b>	Specifies the value with which the contents of the current counter are compared to decide if a counter event should be raised. <ul style="list-style-type: none"> <li><i>entry-value</i>—Entry counter value. Number in the range from -2147483648 to 2147483647, inclusive.</li> </ul>
<b>exit-op</b>	(Optional) Compares the contents of the current counter with the exit value using the specified operator. If there is a match, an event is triggered and event monitoring is reenabled. The <i>operator</i> argument takes one of the following values: <ul style="list-style-type: none"> <li><b>gt</b>—Greater than.</li> <li><b>ge</b>—Greater than or equal to.</li> <li><b>eq</b>—Equal to.</li> <li><b>ne</b>—Not equal to.</li> <li><b>lt</b>—Less than.</li> <li><b>le</b>—Less than or equal to.</li> </ul>
<b>exit-val</b>	(Optional) Specifies the value with which the contents of the current counter are compared to decide whether the exit criteria are met. <ul style="list-style-type: none"> <li><i>exit-value</i>—Exit counter value. Number in the range from -2147483648 to 2147483647, inclusive.</li> </ul>

**Defaults** No EEM events are triggered on the basis of a named counter crossing a threshold.

**Command Modes** Applet configuration

Command History	Release	Modification
	12.2(25)S	This command was introduced.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

**Usage Guidelines** An EEM event is triggered when the value of a specified counter crosses a defined threshold. Depending on the operator, the threshold may be crossed when the value is greater than the threshold or when the value is less than the threshold.

Use the **event counter** command with the **action counter** command when an event occurs periodically and you want an action to be implemented after a specified number of occurrences of the event.

Exit criteria are optional. If exit criteria are not specified, event monitoring will be reenabled immediately. If exit criteria are specified, event monitoring is not reenabled until the criteria are met.

**Examples** The following example shows a policy—EventCounter\_A—that is configured to run once a minute and to increment a well-known counter called critical\_errors. A second policy—EventCounter\_B—is registered to be triggered when the well-known counter called critical\_errors exceeds a threshold of 3. When policy EventCounter\_B runs, it resets the counter back to 0.

```
Router(config)# event manager applet EventCounter_A
Router(config-applet)# event timer watchdog time 60.0
Router(config-applet)# action 1.0 syslog msg "EventCounter_A"
Router(config-applet)# action 2.0 counter name critical_errors value 1 op inc
Router(config-applet)# exit
Router(config)# event manager applet EventCounter_B
Router(config-applet)# event counter name critical_errors entry-op gt entry-val 3 exit-op
lt exit-val 3
Router(config-applet)# action 1.0 syslog msg "EventCounter_B"
Router(config-applet)# action 2.0 counter name critical_errors value 0 op set
```

Related Commands	Command	Description
	<b>action counter</b>	Sets or modifies a named counter when an Embedded Event Manager applet is triggered.
	<b>event manager applet</b>	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

## event interface

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of a generic interface counter crossing a threshold or reaching exit criteria, use the **event interface** command in applet configuration mode. To remove the interface event criteria, use the **no** form of this command.

```
event interface name interface-type interface-number parameter counter-name entry-op operator
entry-val entry-value entry-val-is-increment {true | false} [exit-comb {or | and}] [exit-op
operator exit-val exit-value] [exit-val-is-increment {true | false}] [exit-time exit-time-value]
poll-interval poll-int-value
```

```
no event interface name interface-type interface-number parameter counter-name entry-op
operator entry-val entry-value entry-val-is-increment {true | false} [exit-comb {or | and}]
[exit-op operator exit-val exit-value] [exit-val-is-increment {true | false}] [exit-time
exit-time-value] poll-interval poll-int-value
```

### Syntax Description

<b>name</b>	Specifies the type and number of the interface to monitor. <ul style="list-style-type: none"> <li><i>interface-type interface-number</i>—Interface type and number. For example, FastEthernet 0/1.</li> </ul>
<b>parameter</b>	Specifies the name of the counter to monitor. Supported values for the <i>counter-name</i> argument are one of the following: <ul style="list-style-type: none"> <li><b>input_errors</b>—Includes runts, giants, no buffer, cyclic redundancy checksum (CRC), frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased. Some datagrams may have more than one error.</li> <li><b>input_errors_crc</b>—Number of packets with a CRC generated by the originating LAN station or remote device that do not match the checksum calculated from the data received.</li> <li><b>input_errors_frame</b>—Number of packets received incorrectly that have a CRC error and a noninteger number of octets.</li> <li><b>input_errors_overrun</b>—Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.</li> <li><b>input_packets_dropped</b>—Number of packets dropped because of a full input queue.</li> <li><b>interface_resets</b>—Number of times an interface has been completely reset.</li> <li><b>output_buffer_failures</b>—Number of failed buffers and number of buffers swapped out.</li> <li><b>output_buffer_swappedout</b>—Number of packets swapped to DRAM.</li> <li><b>output_errors</b>—Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the output errors because some datagrams may have more than one error and other datagrams may have errors that do not fall into any of the specifically tabulated categories.</li> </ul>

- **output\_errors\_underrun**—Number of times that the transmitter has been running faster than the router can handle.
- **output\_packets\_dropped**—Number of packets dropped because of a full output queue.
- **receive\_broadcasts**—Number of broadcast or multicast packets received by the interface.
- **receive\_giants**—Number of packets that are discarded because they exceed the maximum packet size of the medium.
- **receive\_rate\_bps**—Interface receive rate, in bytes per second.
- **receive\_rate\_pps**—Interface receive rate, in packets per second.
- **receive\_runts**—Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
- **receive\_throttle**—Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
- **reliability**—Reliability of the interface, as a fraction of 255 (255 out of 255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
- **rxload**—Receive rate of the interface, as a fraction of 255 (255 out of 255 is 100 percent).
- **transmit\_rate\_bps**—Interface transmit rate, in bytes per second.
- **transmit\_rate\_pps**—Interface transmit rate, in packets per second.
- **txload**—Transmit rate of the interface, as a fraction of 255 (255 out of 255 is 100 percent).

**entry-op** Compares the current interface counter value with the entry value using the specified operator. If there is a match, an event is triggered and event monitoring is disabled until the exit criteria are met. The *operator* argument takes one of the following values:

- **gt**—Greater than.
- **ge**—Greater than or equal to.
- **eq**—Equal to.
- **ne**—Not equal to.
- **lt**—Less than.
- **le**—Less than or equal to.

**entry-val** Specifies the value with which the current interface counter value is compared to decide if the interface event should be raised.

- *entry-value*—Entry value. Number in the range from -2147483648 to 2147483647, inclusive.

**entry-val-is-increment** Indicates whether the *entry-value* is an absolute or an increment value.

- If the **true** keyword is specified, the *entry-value* is an increment and the interface event is raised whenever the increment value occurs.
- If the **false** keyword is specified, the *entry-value* is an absolute value and the interface event is raised whenever the absolute value occurs. This is the default.

<b>exit-comb</b>	<p>(Optional) Indicates the combination of exit conditions that must be met before event monitoring is reenabled.</p> <ul style="list-style-type: none"> <li>• If the <b>or</b> operator is specified, an exit comparison operator and an exit object ID value, or an exit time value must exist.</li> <li>• If the <b>and</b> operator is specified, an exit comparison operator, an exit object ID value, and an exit time value must exist.</li> </ul>
<b>exit-op</b>	<p>(Optional) Compares the contents of the current interface counter value with the exit value using the specified operator. If there is a match, an event is triggered and event monitoring is reenabled. The <i>operator</i> argument takes one of the following values:</p> <ul style="list-style-type: none"> <li>• <b>gt</b>—Greater than.</li> <li>• <b>ge</b>—Greater than or equal to.</li> <li>• <b>eq</b>—Equal to.</li> <li>• <b>ne</b>—Not equal to.</li> <li>• <b>lt</b>—Less than.</li> <li>• <b>le</b>—Less than or equal to.</li> </ul>
<b>exit-val</b>	<p>(Optional) Specifies the value with which the contents of the current interface counter value are compared to decide whether the exit criteria are met. If an exit value is specified, you must configure an exit operator.</p> <ul style="list-style-type: none"> <li>• <i>exit-value</i>—Exit value. Number in the range from –2147483648 to 2147483647, inclusive.</li> </ul>
<b>exit-val-is-increment</b>	<p>(Optional) Indicates whether the <i>exit-value</i> is an absolute or an increment value.</p> <ul style="list-style-type: none"> <li>• If the <b>true</b> keyword is specified, the <i>exit-value</i> is an increment and the event monitoring is reenabled whenever the increment value occurs.</li> <li>• If the <b>false</b> keyword is specified, the <i>exit-value</i> is an absolute value and the event monitoring is reenabled whenever the absolute value occurs. This is the default.</li> </ul>
<b>exit-time</b>	<p>(Optional) Specifies the time period after which the event monitoring is reenabled. The timing starts after the event is triggered.</p> <ul style="list-style-type: none"> <li>• <i>exit-time-value</i>—Number that represents seconds and optional milliseconds in the format <i>sssss[.mmm]</i>. The range for seconds is from 0 to 4294967295. The range for milliseconds is from 0 to 999. If using milliseconds only, specify the milliseconds in the format <i>0.mmm</i>.</li> </ul>
<b>poll-interval</b>	<p>Specifies the time interval between consecutive polls.</p> <ul style="list-style-type: none"> <li>• <i>poll-int-value</i>—Number that represents seconds and optional milliseconds in the format <i>sssss[.mmm]</i>. The range for seconds is from 1 to 4294967295. The range for milliseconds is from 0 to 999. If using milliseconds, specify the milliseconds in the format <i>1.mmm</i>. The minimum polling interval is 1 second.</li> </ul>

#### Defaults

No EEM events are triggered on the basis of a generic interface counter crossing a threshold or reaching exit criteria.

**Command Modes** Applet configuration

Command History	Release	Modification
	12.2(25)S	This command was introduced.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

**Usage Guidelines** An EEM event is triggered when one of the fields specified by an interface counter crosses a defined threshold.

Exit criteria are optional. If exit criteria are not specified, event monitoring will be reenabled immediately. If exit criteria are specified—on the basis of values or time periods—event monitoring is not reenabled until the criteria are met.

**Examples** The following example shows how a policy named EventInterface is triggered every time the receive\_throttle counter for the FastEthernet0/0 interface is incremented by 5. The polling interval to check the counter is specified to run once every 10 seconds.

```
Router(config)# event manager applet EventInterface
Router(config-applet)# event interface name FastEthernet0/0 parameter receive_throttle
entry-op ge entry-val 5 entry-val-is-increment true poll-interval 10
Router(config-applet)# action 1.0 syslog msg "Applet EventInterface"
```

Related Commands	Command	Description
	<b>event manager applet</b>	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

# event ioswdsysmon

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of Cisco IOS system monitor counters crossing a threshold, use the **event ioswdsysmon** command in applet configuration mode. To remove the event criteria, use the **no** form of this command.

```
event ioswdsysmon sub1 subevent1 [timewin timewin-value] [sub12-op {and | or | andnot} sub2
subevent2]
```

```
no event ioswdsysmon sub1 subevent1 [timewin timewin-value] [sub12-op {and | or | andnot}
sub2 subevent2]
```

Subevent Syntax (for the *subevent1* and *subevent2* Arguments)

```
cpu-proc taskname process-name op operator val value [period period-value]
```

```
mem-proc taskname process-name op operator val value [is-percent {true | false}] [period
period-value]
```

## Syntax Description

<b>sub1</b>	Specifies the first subevent. <ul style="list-style-type: none"> <li><i>subevent1</i>—First subevent. Use one of the two forms of syntax shown above under the Subevent Syntax heading.</li> </ul>
<b>timewin</b>	(Optional) Specifies the time window within which all of the subevents must occur in order for an event to be generated. <ul style="list-style-type: none"> <li><i>timewin-value</i>—Number that represents seconds and optional milliseconds in the format <i>sssss[.mmm]</i>. The range for seconds is from 0 to 4294967295. The range for milliseconds is from 0 to 999. If using milliseconds only, specify the milliseconds in the format <i>0.mmm</i>.</li> </ul>
<b>sub12-op</b>	(Optional) Indicates the combination operator for comparison between subevent 1 and subevent 2. <ul style="list-style-type: none"> <li>If the <b>and</b> operator is specified, both the results of subevent 1 and subevent 2 must cross the specified thresholds.</li> <li>If the <b>or</b> operator is specified, the results of either subevent 1 or subevent 2 must cross the specified thresholds.</li> <li>If the <b>andnot</b> operator is specified, only the results from subevent 1 must cross the specified threshold.</li> </ul>
<b>sub2</b>	(Optional) Specifies the second subevent. <ul style="list-style-type: none"> <li><i>subevent2</i>—Second subevent. Use one of the two forms of syntax shown above under the Subevent Syntax heading.</li> </ul>
<b>cpu-proc</b>	Specifies the use of a sample collection of CPU statistics.
<b>mem-proc</b>	Specifies the use of a sample collection of memory statistics.
<b>taskname</b>	Specifies a process name. <ul style="list-style-type: none"> <li><i>process-name</i>—Name of the Cisco IOS process to be monitored. If the process name contains embedded blanks, enclose it in double quotation marks.</li> </ul>

<b>op</b>	<p>Compares the collected CPU or memory usage sample with the value specified in the <i>value</i> argument. If there is a match, the subevent is triggered. The <i>operator</i> argument takes one of the following values:</p> <ul style="list-style-type: none"> <li>• <b>gt</b>—Greater than.</li> <li>• <b>ge</b>—Greater than or equal to.</li> <li>• <b>eq</b>—Equal to.</li> <li>• <b>ne</b>—Not equal to.</li> <li>• <b>lt</b>—Less than.</li> <li>• <b>le</b>—Less than or equal to.</li> </ul>
<b>val</b>	<p>Specifies the value with which the collected CPU or memory usage sample is compared to decide if the subevent should be raised.</p> <ul style="list-style-type: none"> <li>• <i>value</i>—Number in the range from 1 to 4294967295.</li> </ul>
<b>period</b>	<p>(Optional) Specifies the elapsed time period for the collection samples to be averaged.</p> <ul style="list-style-type: none"> <li>• <i>period-value</i>—Number that represents seconds and optional milliseconds in the format <i>sssss[.mmm]</i>. The range for seconds is from 0 to 4294967295. The range for milliseconds is from 0 to 999. If using milliseconds only, specify the milliseconds in the format <i>0.mmm</i>. If the time period is 0, the most recent sample is used.</li> </ul>
<b>is-percent</b>	<p>(Optional) Indicates whether the <i>value</i> argument is a percentage.</p> <ul style="list-style-type: none"> <li>• If the <b>true</b> keyword is specified, the <i>value</i> argument is a percentage.</li> <li>• If the <b>false</b> keyword is specified, the <i>value</i> argument is not a percentage.</li> </ul>

**Defaults**

No EEM events are triggered on the basis of Cisco IOS system monitor counters.

**Command Modes**

Applet configuration

**Command History**

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

**Usage Guidelines**

An EEM event is triggered when one of the Cisco IOS system monitor counters crosses a defined threshold. Depending on the operator, the threshold may be crossed when the value exceeds the threshold or when the value is less than the threshold.

---

**Examples**

The following example shows how to configure a policy to trigger an applet when the total amount of memory used by the process named “IP RIB Update” has increased by more than 50 percent over the sample period of 60 seconds:

```
Router(config)# event manager applet IOSWD_Sample3
Router(config-applet)# event ioswdsysmon sub1 mem-proc taskname "IP RIB Update" op gt val
50 is-percent true period 60
Router(config-applet)# action 1 syslog msg "IOSWD_Sample3 Policy Triggered"
```

---

**Related Commands**

Command	Description
<b>event manager applet</b>	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

# event manager applet

To register an applet with the Embedded Event Manager (EEM) and to enter applet configuration mode, use the **event manager applet** command in global configuration mode. To remove the applet command from the configuration file, use the **no** form of this command.

**event manager applet** *applet-name*

**no event manager applet** *applet-name*

## Syntax Description

<i>applet-name</i>	Name of the applet file.
--------------------	--------------------------

## Defaults

No EEM applets are registered.

## Command Modes

Global configuration

## Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

## Usage Guidelines

An EEM applet is a concise method for defining event screening criteria and the actions to be taken when that event occurs.

Only one event configuration command is allowed within an applet configuration. When applet configuration submode is exited and no event command is present, a warning is displayed stating that no event is associated with this applet. If no event is specified, this applet is not considered registered and the applet is not displayed. When no action is associated with this applet, events are still triggered but no actions are performed. Multiple action applet configuration commands are allowed within an applet configuration. Use the **show event manager policy registered** command to display a list of registered applets.

Before modifying an EEM applet, use the **no** form of this command to unregister the applet because the existing applet is not replaced until you exit applet configuration mode. While you are in applet configuration mode modifying the applet, the existing applet may be executing. When you exit applet configuration mode, the old applet is unregistered and the new version is registered.

Action configuration commands are uniquely identified using the *label* argument, which can be any string value. Actions are sorted in ascending alphanumeric key sequence using the *label* argument as the sort key and are run using this sequence.

The EEM schedules and runs policies on the basis of an event specification that is contained within the policy itself. When applet configuration mode is exited, EEM examines the event and action commands that are entered and registers the applet to be run when a specified event occurs.

## Examples

The following example shows an EEM applet called IPSLAping1 being registered to run when there is an exact match on the value of a specified SNMP object ID that represents a successful IP SLA ICMP echo operation (this is equivalent to a **ping** command). Four actions are triggered when the echo operation fails, and event monitoring is disabled until after the second failure. A message saying that the ICMP echo operation to a server failed is sent to syslog, an SNMP trap is generated, EEM publishes an application-specific event, and a counter called IPSLA1F is incremented by a value of one.

```
Router(config)# event manager applet IPSLAping1
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.42.1.2.9.1.6.4 get-type exact
entry-op eq entry-val 1 exit-op eq exit-val 2 poll-interval 5
Router(config-applet)# action 1.0 syslog priority critical msg "Server IP echo failed:
OID=$_snmp_oid_val"
Router(config-applet)# action 1.1 snmp-trap strdata "EEM detected server reachability
failure to 10.1.88.9"
Router(config-applet)# action 1.2 publish-event sub-system 88000101 type 1 arg1 10.1.88.9
arg2 IPSLAEcho arg3 fail
Router(config-applet)# action 1.3 counter name _IPSLA1F value 1 op inc
```

## Related Commands

Command	Description
<b>show event manager policy registered</b>	Displays registered Embedded Event Manager policies.

# event manager directory user

To specify a directory to use for storing user library files or user-defined Embedded Event Manager (EEM) policies, use the **event manager directory user** command in global configuration command. To disable use of a directory for storing user library files or user-defined EEM policies, use the **no** form of this command.

**event manager directory user** {*library path* | *policy path*}

**no event manager directory user** {*library path* | *policy path*}

Syntax Description	library	Specifies using the directory to store user library files.
	<b>policy</b>	Specifies using the directory to store user-defined EEM policies.
	<i>path</i>	The absolute pathname to the user directory on the flash device.

**Defaults** No directory is specified for storing user library files or user-defined EEM policies.

**Command Modes** Global configuration

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

**Usage Guidelines** The user library directory is needed to store user library files associated with authoring EEM policies. If you have no plans to author EEM policies, you need not create a user library directory.

Modular Cisco IOS software supports policy files created by using the Tool Command Language (Tcl) scripting language. Tcl is provided in the Modular Cisco IOS software image when the EEM is installed on the network device. Files with the .tcl extension can be EEM policies, Tcl library files, or a special Tcl library index file named "tclindex." The tclindex file contains a list of user function names and the library files that contain the user functions. The EEM searches the user library directory when Tcl starts up to process the tclindex file.

To create the user library directory before identifying it to the EEM, use the **mkdir** command in privileged EXEC mode. After creating the user library directory, you can use the **copy** command to copy .tcl library files into the user library directory.

The user policy directory is needed to store user-defined policy files. If you have no plans to author EEM policies, you need not create a user policy directory. The EEM searches the user policy directory when you enter the **event manager policy *policy-filename* type user** command.

To create the user policy directory before identifying it to the EEM, use the **mkdir** command in privileged EXEC mode. After creating the user policy directory, you can use the **copy** command to copy policy files into the user policy directory.

---

**Examples**

The following example shows how to specify disk0:/user\_library as the directory to use for storing user library files:

```
Router(config)# event manager directory user library disk0:/user_library
```

---

**Related Commands**

Command	Description
<b>copy</b>	Copies any file from a source to a destination.
<b>event manager policy</b>	Registers an EEM policy with the EEM.
<b>mkdir</b>	Creates a new directory in a Class C flash file system.

# event manager environment

To set an Embedded Event Manager (EEM) environment variable, use the **event manager environment** command in global configuration mode. To disable an EEM environment variable, use the **no** form of this command.

**event manager environment** *variable-name string*

**no event manager environment** *variable-name*

## Syntax Description

<i>variable-name</i>	Name assigned to the EEM environment variable.
<i>string</i>	Series of characters, including embedded spaces, to be placed in the environment variable <i>variable-name</i> .

## Defaults

No EEM environment variables are set.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

## Usage Guidelines

By convention, the names of all environment variables defined by Cisco begin with an underscore character to set them apart: for example, `_show_cmd`.

To support embedded white spaces in the *string* argument, the current implementation of this command interprets everything after the *variable-name* argument to the end of the line to be part of the *string* argument.

To display the name and value of all EEM environment variables after you have configured them, use the **show event manager environment** command.

## Examples

The following example of the **event manager environment** command defines a set of EEM environment variables:

```
Router(config)# event manager environment _cron_entry 0-59/2 0-23/1 * * 0-7
Router(config)# event manager environment _show_cmd show version
```

## Related Commands

Command	Description
<b>show event manager environment</b>	Displays the name and value of all EEM environment variables.

# event manager history size

To change the size of Embedded Event Manager (EEM) history tables, use the **event manager history size** command in global configuration mode. To restore the default history table size, use the **no** form of this command.

```
event manager history size {events | traps} [size]
```

```
no event manager history size {events | traps}
```

Syntax Description	events	Changes the size of the EEM event history table.
	traps	Changes the size of the EEM Simple Network Management Protocol (SNMP) trap history table.
	size	(Optional) Number of history table entries. Range is from 1 to 50. Default is 50.

**Defaults** The size of the history table is 50 entries.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(25)S	This command was introduced.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

**Examples** The following example of the **event manager history size** command changes the size of the SNMP trap history table to 30 entries:

```
Router(config)# event manager history size traps 30
```

Related Commands	Command	Description
	<b>show event manager history events</b>	Displays the EEM events that have been triggered.
	<b>show event manager history traps</b>	Displays the EEM SNMP traps that have been sent.

# event manager policy

To register an Embedded Event Manager (EEM) policy with the EEM, use the **event manager policy** command in global configuration mode. To remove the **event manager policy** command from the configuration file, use the **no** form of this command.

**event manager policy** *policy-filename* [**type** {**system** | **user**}] [**trap**]

**no event manager policy** *policy-filename*

## Syntax Description

<i>policy-filename</i>	Name of the policy file.
<b>type</b>	(Optional) Specifies the type of EEM policy to be registered.
<b>system</b>	(Optional) Registers a Cisco-defined system policy.
<b>user</b>	(Optional) Registers a user-defined policy.
<b>trap</b>	(Optional) Generates a Simple Network Management Protocol (SNMP) trap when the policy is triggered.

## Defaults

No EEM policies are registered.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	The <b>user</b> keyword was added, and this command was integrated into Cisco IOS Release 12.3(14)T.

## Usage Guidelines

The EEM schedules and runs policies on the basis of an event specification that is contained within the policy itself. When the **event manager policy** command is invoked, the EEM examines the policy and registers it to be run when the specified event occurs.

If you enter the **event manager policy** command without specifying the optional **type** keyword, the EEM first tries to locate the specified policy file in the system policy directory. If the EEM finds the file in the system policy directory, it registers the policy as a system policy. If the EEM does not find the specified policy file in the system policy directory, it looks in the user policy directory. If the EEM locates the specified file in the user policy directory, it registers the policy file as a user policy. If the EEM finds policy files with the same name in both the system policy directory and the user policy directory, the policy file in the system policy directory takes precedence and is registered as a system policy.

## Examples

The following example of the **event manager policy** command registers a system-defined policy named `tm_countdown_ios.tcl` located in the system policy directory:

```
Router(config)# event manager policy tm_countdown_ios.tcl type system
```

The following example of the **event manager policy** command registers a user-defined policy named `cron.tcl` located in the user policy directory:

```
Router(config)# event manager policy cron.tcl type user
```

---

**Related Commands**

Command	Description
<b>show event manager policy registered</b>	Displays registered EEM policies.

# event manager run

To manually run a registered Embedded Event Manager (EEM) policy, use the **event manager run** command in global configuration mode.

**event manager run** *policy-filename*

<b>Syntax Description</b>	<i>policy-filename</i>	Name of the policy file.
---------------------------	------------------------	--------------------------

**Defaults** No registered EEM policies are run.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(14)T	This command was introduced.

**Usage Guidelines** EEM usually schedules and runs policies on the basis of an event specification that is contained within the policy itself. The **event manager run** command allows policies to be run manually. Before this command is used, the **event none** command must be configured in applet configuration for the specified policy to indicate to EEM that the policy is to be run manually.

This command does not have a **no** form.

**Examples** The following example of the **event manager run** command manually runs an EEM policy named `policy_manual.tcl`:

```
Router(config)# event manager run policy-manual.tcl
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>event manager applet</b>	Registers an EEM applet with EEM and enters applet configuration mode.
	<b>event manager policy</b>	Registers an EEM policy with EEM.
	<b>event none</b>	Registers an EEM policy with EEM and indicates that the policy may be run manually.
	<b>show event manager policy registered</b>	Displays registered EEM policies.

# event manager scheduler policy suspend

To immediately suspend Embedded Event Manager (EEM) policy scheduling execution, use the **event manager scheduler policy suspend** command in global configuration mode. To resume EEM policy scheduling, use the **no** form of this command.

**event manager scheduler policy suspend**

**no event manager scheduler policy suspend**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Policy scheduling is active.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(25)S	This command was introduced.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

**Usage Guidelines** Use the **event manager scheduler policy suspend** command to suspend all policy scheduling requests and do no scheduling until you enter the **no** form of the command. The **no** form of the command resumes policy scheduling and executes any pending policies.

You might want to suspend policy execution immediately instead of unregistering policies one by one for the following reasons:

- For security—if you think the security of your system has been compromised.
- For performance—if you want to suspend policy execution temporarily to make more CPU cycles available for other functions.

**Examples** The following example of the **event manager scheduler suspend** command disables policy scheduling:

```
Router(config)# event manager scheduler policy suspend
```

```
May 19 14:31:22.439: fm_server[12330]: %HA_EM-6-FMS_POLICY_EXEC: fh_io_msg: Policy execution has been suspended
```

The following example of the **event manager scheduler suspend** command enables policy scheduling:

```
Router(config)# no event manager scheduler policy suspend
```

```
May 19 14:31:40.449: fm_server[12330]: %HA_EM-6-FMS_POLICY_EXEC: fh_io_msg: Policy execution has been resumed
```

Related Commands	Command	Description
	<b>event manager policy</b>	Registers an EEM policy with the EEM.

# event manager scheduler script

To set the Embedded Event Manager (EEM) script scheduling options, use the **event manager scheduler script** command in global configuration mode. To remove the EEM script scheduling options and restore the default value, use the **no** form of this command.

**event manager scheduler script thread class default** *default-number*

**no event manager scheduler script thread class default** *default-number*

<b>Syntax Description</b>	<p><b>thread class default</b> Specifies the number of concurrent script execution threads. Each script execution thread is used by one EEM policy as it executes.</p> <ul style="list-style-type: none"> <li><i>default-number</i>—Number of concurrent script execution threads. Default is one script execution thread.</li> </ul>
---------------------------	---

<b>Defaults</b>	Only one EEM policy can be run at a time.
-----------------	---

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.3(14)T</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.3(14)T	This command was introduced.
Release	Modification				
12.3(14)T	This command was introduced.				

<b>Usage Guidelines</b>	Use the <b>event manager scheduler script</b> command if you want more than one EEM policy to run concurrently.
-------------------------	---

<b>Examples</b>	<p>The following example shows how to specify two script execution threads to run concurrently:</p> <pre>Router(config)# event manager scheduler script thread class default 2</pre>
-----------------	--

# event manager session cli username

To associate a username with Embedded Event Manager (EEM) policies that use the command-line interface (CLI) library, use the **event manager session cli username** command in global configuration mode. To remove the username association with EEM policies that use the CLI library, use the **no** form of this command.

**event manager session cli username** *username*

**no event manager session cli username** *username*

<b>Syntax Description</b>	<i>username</i>	Username assigned to EEM CLI sessions that are initiated by EEM policies.
---------------------------	-----------------	---

<b>Defaults</b>	No username is associated with EEM CLI sessions.
-----------------	--

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(14)T	This command was introduced.

<b>Usage Guidelines</b>	<p>Use the <b>event manager session cli username</b> command to assign a username for EEM policy CLI sessions when TACACS+ is used for command authorization.</p> <p>If you are using authentication, authorization, and accounting (AAA) security and implement authorization on a command basis, you should use the <b>event manager session cli username</b> command to set a username to be associated with a Tool Command Language (Tcl) session. The username is used when a Tcl policy executes a CLI command. TACACS+ verifies each CLI command using the username associated with the Tcl session that is running the policy. Commands from Tcl policies are not usually verified because the router must be in privileged EXEC mode to register the policy.</p>
-------------------------	---

<b>Examples</b>	<p>The following example of the <b>event manager session cli username</b> command associates the username eemuser with EEM CLI sessions initiated by EEM policies:</p>
-----------------	--

```
Router(config)# event manager session cli username financel
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show event manager session cli username</b>	Displays the username associated with CLI sessions initiated by EEM policies that use the EEM CLI library.

## event none

To specify that an Embedded Event Manager (EEM) policy is to be registered with the EEM and can be run manually, use the **event none** command in applet configuration mode. To remove the **event none** command from the configuration file, use the **no** form of this command.

**event none** *policy-filename*

**no event none** *policy-filename*

Syntax Description	<i>policy-filename</i>	Name of the policy file.
--------------------	------------------------	--------------------------

**Defaults** No EEM policies are specified to be run manually.

**Command Modes** Applet configuration

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

**Usage Guidelines** EEM usually schedules and runs policies on the basis of an event specification that is contained within the policy itself. The **event none** command allows EEM to identify an EEM policy that can either be run manually or be run when an EEM applet is triggered. To run the policy, use either the **action policy** command in applet configuration mode or the **event manager run** command in global configuration mode.

**Examples** The following example shows how to register a policy named manual-policy to be run manually and then how to execute the policy:

```
Router(config)# event manager applet manual-policy
Router(config-applet)# event none manual-policy
Router(config-applet)# exit
Router(config)# event manager run manual-policy
```

Related Commands	Command	Description
	<b>action policy</b>	Registers an EEM policy with EEM.
	<b>event manager applet</b>	Registers an EEM applet with EEM and enters applet configuration mode.
	<b>event manager run</b>	Manually runs a registered EEM policy.
	<b>show event manager policy registered</b>	Displays registered EEM policies.

# event oir

To specify that an Embedded Event Manager (EEM) applet be run on the basis of an event raised when a hardware card online insertion and removal (OIR) occurs, use the **event oir** command in applet configuration mode. To remove the **event oir** command from the configuration, use the **no** form of this command.

**event oir**

**no event oir**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No EEM applets are run on the basis of an OIR event.

**Command Modes** Applet configuration

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

**Examples** The following example shows how to configure an EEM applet to be run on the basis of an OIR event:

```
Router(config)# event manager applet oir-event
Router(config-applet)# event oir
Router(config-applet)# exit
```

Related Commands	Command	Description
	<b>event manager applet</b>	Registers an EEM applet with EEM and enters applet configuration mode.

## event snmp

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run by sampling Simple Network Management Protocol (SNMP) object identifier values, use the **event snmp** command in applet configuration mode. To remove the SNMP event criteria, use the **no** form of this command.

```
event snmp oid oid-value get-type {exact | next} entry-op operator entry-val entry-value
[entry-type {value | increment | rate}] [exit-comb {or | and}] [exit-op operator] [exit-val
exit-value] [exit-type {value | increment | rate}] [exit-time exit-time-value] [exit-event
{true | false}] [average-factor average-factor-value] poll-interval poll-int-value
```

```
no event snmp oid oid-value get-type {exact | next} entry-op operator entry-val entry-value
[entry-type {value | increment | rate}] [exit-comb {or | and}] [exit-op operator] [exit-val
exit-value] [exit-type {value | increment | rate}] [exit-time exit-time-value] [exit-event
{true | false}] [average-factor average-factor-value] poll-interval poll-int-value
```

---

### Syntax Description

<b>oid</b>	<p>Specifies the SNMP object identifier (object ID) values in the <i>oid-value</i> argument as the event criteria.</p> <p><i>oid-value</i>—Object ID value of the data element, in SNMP dotted notation. An OID is defined as a type in the associated MIB, CISCO-EMBEDDED-EVENT-MGR-MIB, and each type has an object value. Monitoring of some OID types is supported. An error message is returned if the OID is not one of the following:</p> <ul style="list-style-type: none"> <li>• INTEGER_TYPE</li> <li>• COUNTER_TYPE</li> <li>• GAUGE_TYPE</li> <li>• TIME_TICKS_TYPE</li> <li>• COUNTER_64_TYPE</li> <li>• OCTET_PRIM_TYPE</li> <li>• OPAQUE_PRIM_TYPE</li> </ul>
<b>get-type</b>	<p>Specifies the type of SNMP get operation to be applied to the object ID specified by the <i>oid-value</i> argument.</p> <ul style="list-style-type: none"> <li>• <b>exact</b>—Retrieves the object ID specified by the <i>oid-value</i> argument.</li> <li>• <b>next</b>—Retrieves the object ID that is the alphanumeric successor to the object ID specified by the <i>oid-value</i> argument.</li> </ul>

---

<b>entry-op</b>	<p>Compares the contents of the current object ID with the entry value using the specified operator. If there is a match, an event is triggered and event monitoring is disabled until the exit criteria are met. The <i>operator</i> argument takes one of the following values:</p> <ul style="list-style-type: none"> <li>• <b>gt</b>—Greater than.</li> <li>• <b>ge</b>—Greater than or equal to.</li> <li>• <b>eq</b>—Equal to.</li> <li>• <b>ne</b>—Not equal to.</li> <li>• <b>lt</b>—Less than.</li> <li>• <b>le</b>—Less than or equal to.</li> </ul>
<b>entry-val</b>	<p>Specifies the value with which the contents of the current object ID are compared to decide if an SNMP event should be raised.</p> <ul style="list-style-type: none"> <li>• <i>entry-value</i>—Entry object ID value of the data element.</li> </ul>
<b>entry-type</b>	<p>(Optional) Specifies a type of operation to be applied to the object ID specified by the <i>entry-value</i> argument. If not specified, the value is assumed.</p> <ul style="list-style-type: none"> <li>• If the <b>value</b> keyword is specified, an SNMP event should be raised on the basis of a comparison of the absolute value of the <i>entry-value</i> argument.</li> <li>• If the <b>increment</b> keyword is specified, an SNMP event should be raised on the basis of a comparison of the incremental value of the <i>entry-value</i> argument since the last poll interval.</li> <li>• If the <b>rate</b> keyword is specified, an SNMP event should be raised on the basis of a comparison of the rate of change of the <i>entry-value</i> argument over a period. Rate is defined to be the sum of the incremental difference for the sample taken at each poll interval as compared to the previous sample divided by the period. The period is defined as the average factor times the poll interval. An event is triggered on the basis of a comparison of the derived rate value.</li> </ul> <p><b>Note</b> The increment and rate types are supported only for the following OID types: INTEGER_TYPE, COUNTER_TYPE, and COUNTER_64_TYPE.</p>
<b>exit-comb</b>	<p>(Optional) Indicates the combination of exit conditions that must be met before event monitoring is reenabled.</p> <ul style="list-style-type: none"> <li>• If the <b>or</b> operator is specified, an exit comparison operator and an exit object ID value or an exit time value must exist.</li> <li>• If the <b>and</b> operator is specified, an exit comparison operator, an exit object ID value, and an exit time value must exist.</li> </ul>

<b>exit-op</b>	<p>(Optional) Compares the contents of the current object ID with the exit value using the specified operator. If there is a match, an event is triggered and event monitoring is reenabled. The <i>operator</i> argument takes one of the following values:</p> <ul style="list-style-type: none"> <li>• <b>gt</b>—Greater than.</li> <li>• <b>ge</b>—Greater than or equal to.</li> <li>• <b>eq</b>—Equal to.</li> <li>• <b>ne</b>—Not equal to.</li> <li>• <b>lt</b>—Less than.</li> <li>• <b>le</b>—Less than or equal to.</li> </ul>
<b>exit-val</b>	<p>(Optional) Specifies the value with which the contents of the current object ID are compared to decide whether the exit criteria are met.</p> <ul style="list-style-type: none"> <li>• <i>exit-value</i>—Exit object ID value of the data element.</li> </ul>
<b>exit-type</b>	<p>(Optional) Specifies a type of operation to be applied to the object ID specified by the <i>exit-value</i> argument. If not specified, the value is assumed.</p> <ul style="list-style-type: none"> <li>• If the <b>value</b> keyword is specified, event monitoring will be reenabled on the basis of a comparison of the absolute value of the <i>exit-value</i> argument.</li> <li>• If the <b>increment</b> keyword is specified, event monitoring will be reenabled on the basis of a comparison of the incremental value of the <i>exit-value</i> argument since the last poll interval.</li> <li>• If the <b>rate</b> keyword is specified, event monitoring will be reenabled on the basis of a comparison of the rate of change of the <i>exit-value</i> argument over a period. Rate is defined to be the sum of the incremental difference for the sample taken at each poll interval as compared to the previous sample divided by the period. The period is defined as the average factor times the poll interval. Event monitoring will be reenabled on the basis of a comparison of the derived rate value.</li> </ul> <p><b>Note</b> The increment and rate types are supported only for the following OID types: INTEGER_TYPE, COUNTER_TYPE, and COUNTER_64_TYPE.</p>
<b>exit-time</b>	<p>(Optional) Specifies the time period after which the event monitoring is reenabled. The timing starts after the event is triggered.</p> <ul style="list-style-type: none"> <li>• <i>exit-time-value</i>—Number that represents seconds and optional milliseconds in the format ssssss[.mmm]. The range for seconds is from 0 to 4294967295. The range for milliseconds is from 0 to 999. If using milliseconds only, specify the milliseconds in the format 0.mmm.</li> </ul>
<b>exit-event</b>	<p>(Optional) Indicates whether a separate exit event is to be triggered when event monitoring is enabled after an initial event is triggered.</p> <ul style="list-style-type: none"> <li>• If the <b>true</b> keyword is specified, a separate exit event is triggered.</li> <li>• If the <b>false</b> keyword is specified, a separate exit event is not triggered. This is the default.</li> </ul>

<b>average-factor</b>	(Optional) Specifies a number used to calculate the period used for rate-based calculations. The <i>average-factor-value</i> is multiplied by the <i>poll-int-value</i> to derive the period in milliseconds. <ul style="list-style-type: none"> <li><i>average-factor-value</i>—Number in the range from 1 to 64. The minimum average factor value is 1.</li> </ul>
<b>poll-interval</b>	Specifies the time interval between consecutive polls. <ul style="list-style-type: none"> <li><i>poll-int-value</i>—Number that represents seconds and optional milliseconds in the format sssss[.mmm]. The range for seconds is from 1 to 4294967295. The range for milliseconds is from 0 to 999. The minimum polling interval is 1 second.</li> </ul>

**Defaults**

No EEM events are triggered on the basis of SNMP object identifier values.

**Command Modes**

Applet configuration

**Command History**

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	Optional keywords to support SNMP rate-based events were added.

**Usage Guidelines**

An EEM event is triggered when one of the fields specified by an SNMP object ID crosses a defined threshold. If multiple conditions exist, the SNMP event will be triggered when all the conditions are met.

Exit criteria are optional. If exit criteria are not specified, event monitoring will be reenabled immediately. If exit criteria are specified—on the basis of values or time periods—event monitoring is not reenabled until the criteria are met.

**Examples**

The following example shows how an EEM applet called memory-fail will run when there is an exact match on the value of a specified SNMP object ID that represents the amount of current process memory. A message saying that process memory is exhausted and noting the current available memory will be sent to syslog.

```
Router(config)# event manager applet memory-fail
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op
lt entry-val 5120000 poll-interval 10
Router(config-applet)# action 1.0 syslog msg "Memory exhausted; current available memory
is $_snmp_oid_val bytes"
```

The following example shows an EEM applet called IPSLAping1 being registered to run when there is an exact match on the value of a specified SNMP object ID that represents a successful IP SLA ICMP echo operation (this is equivalent to a **ping** command). Four actions are triggered when the echo operation fails, and event monitoring is disabled until after the second failure. A message saying that the ICMP echo operation to a server failed is sent to syslog, an SNMP trap is generated, EEM publishes an application-specific event, and a counter called IPSLA1F is incremented by a value of one.

```
Router(config)# event manager applet IPSLAping1
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.42.1.2.9.1.6.4 get-type exact
entry-op eq entry-val 1 exit-op eq exit-val 2 poll-interval 5
Router(config-applet)# action 1.0 syslog priority critical msg "Server IP echo failed:
OID=$_snmp_oid_val"
Router(config-applet)# action 1.1 snmp-trap strdata "EEM detected server reachability
failure to 10.1.88.9"
Router(config-applet)# action 1.2 publish-event sub-system 88000101 type 1 arg1 10.1.88.9
arg2 IPSLAEcho arg3 fail
Router(config-applet)# action 1.3 counter name _IPSLA1F value 1 op inc
```

#### Related Commands

Command	Description
<b>event manager applet</b>	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

# event syslog

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run by matching syslog messages, use the **event syslog** command in applet configuration mode. To remove the syslog message event criteria, use the **no** form of this command.

**event syslog pattern** *regular-expression* [**occurs** *num-occurrences*] [**period** *period-value*] [**priority** *priority-level*] [*severity-level*]

**no event syslog pattern** *regular-expression* [**occurs** *num-occurrences*] [**period** *period-value*] [**priority** *priority-level*] [*severity-level*]

Syntax Description		
<b>pattern</b>	Specifies the regular expression used to perform the syslog message pattern match.	<ul style="list-style-type: none"> <li><i>regular-expression</i>—Regular expression.</li> </ul>
<b>occurs</b>	(Optional) Specifies the number of matching occurrences before an EEM event is triggered. If a number is not specified, an EEM event is triggered after the first match.	<ul style="list-style-type: none"> <li><i>num-occurrences</i>—The number of occurrences. The value must be greater than 0.</li> </ul>
<b>period</b>	(Optional) Specifies the time interval during which the one or more occurrences must take place. If the keyword is not specified, no time period check is applied.	<ul style="list-style-type: none"> <li><i>period-value</i>—Number that represents seconds and optional milliseconds in the format <i>sssss[.mmm]</i>. The range for seconds is from 0 to 4294967295. The range for milliseconds is from 0 to 999. If using milliseconds only, specify the milliseconds in the format <i>0.mmm</i>.</li> </ul>

<b>priority</b>	<p>(Optional) Specifies the priority level of the syslog messages to be screened. If the keyword is selected, the <i>priority-level</i> argument must be defined. If the keyword is not specified, the software will use the default of <b>priority all</b>, and all priorities will be considered when log messages are screened.</p> <ul style="list-style-type: none"> <li>• <i>priority-level</i>—The number or name of the desired priority level against which syslog messages are matched. Messages at or numerically lower than the specified level are matched. Priority levels are as follows (enter the keyword or number, if available): <ul style="list-style-type: none"> <li>– <b>all</b>—All priorities are considered when log messages are screened.</li> <li>– <b>{0   emergencies}</b>—System is unusable.</li> <li>– <b>{1   alerts}</b>—Immediate action is needed.</li> <li>– <b>{2   critical}</b>—Critical conditions.</li> <li>– <b>{3   errors}</b>—Error conditions.</li> <li>– <b>{4   warnings}</b>—Warning conditions.</li> <li>– <b>{5   notifications}</b>—Normal but significant conditions.</li> <li>– <b>{6   informational}</b>—Informational messages.</li> <li>– <b>{7   debugging}</b>—Debugging messages.</li> </ul> </li> </ul>
<i>severity-level</i>	<p>(Optional) Specifies the severity level of the syslog messages to be screened. If no severity level is specified, the software will not use any severity filtering and all events will be considered when log messages are screened. The <i>severity-level</i> argument may be one or more of the following keywords:</p> <ul style="list-style-type: none"> <li>• <b>severity-critical</b>—Critical conditions.</li> <li>• <b>severity-debugging</b>—Debugging messages.</li> <li>• <b>severity-fatal</b>—Fatal conditions.</li> <li>• <b>severity-major</b>—Major conditions.</li> <li>• <b>severity-minor</b>—Minor conditions.</li> <li>• <b>severity-normal</b>—Normal conditions.</li> <li>• <b>severity-notification</b>—Significant conditions.</li> <li>• <b>severity-warning</b>—Warning conditions.</li> </ul>

**Defaults**

No EEM events are triggered on the basis of matches with syslog messages.

**Command Modes**

Applet configuration

**Command History**

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	Optional severity-level keywords were added.

---

**Usage Guidelines**

Use the **event syslog** command to set up event criteria against which syslog messages are matched. Syslog messages are compared against a specified regular expression. After a specified number of matches occurs within a specified time period, an EEM event is triggered. If multiple conditions exist, the EEM event is triggered when all the conditions are met.

---

**Examples**

The following example shows how to specify an EEM applet to run when syslog identifies that Ethernet interface 1/0 is down. The applet sends a message about the interface to syslog.

```
Router(config)# event manager applet interface-down
Router(config-applet)# event syslog pattern {.*UPDOWN.*Ethernet1/0.*} occurs 4
Router(config-applet)# action 1.0 syslog msg "Ethernet interface 1/0 is down"
```

---

**Related Commands**

Command	Description
<b>event manager applet</b>	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

## event timer

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of time-specific events, use the **event timer** command in applet configuration mode. To remove the time-specific event criteria, use the **no** form of this command.

**event timer** { **absolute time** *time-value* | **countdown time** *time-value* | **cron cron-entry** *cron-entry* | **watchdog time** *time-value* } [**name** *timer-name*]

**no event timer** { **absolute time** *time-value* | **countdown time** *time-value* | **cron cron-entry** *cron-entry* | **watchdog time** *time-value* } [**name** *timer-name*]

Syntax	Description
<b>absolute</b>	Specifies that an event is triggered when the specified absolute time of day occurs.
<b>time</b>	Specifies the time interval during which the event must take place. <ul style="list-style-type: none"> <li><i>time-value</i>—Number that represents seconds and optional milliseconds in the format <i>sssss[.mmm]</i>. The range for seconds is from 0 to 4294967295. The range for milliseconds is from 0 to 999. If using milliseconds only, specify the milliseconds in the format <i>0.mmm</i>.</li> </ul>
<b>countdown</b>	Specifies that an event is triggered when the specified time counts down to zero. The timer does not reset.
<b>cron</b>	Specifies that an event is triggered when the CRON string specification matches the current time.

<b>cron-entry</b>	<p>Specifies the first five fields of a UNIX crontab entry as used with the UNIX CRON daemon.</p> <ul style="list-style-type: none"> <li>• <i>cron-entry</i>—A text string that consists of five fields. The fields represent the time and date when CRON timer events will be triggered; the fields are separated by spaces. Fields and corresponding values are as follows: <ul style="list-style-type: none"> <li>– <i>minute</i>—Minute when a CRON timer event is triggered. Valid entries are numbers in the range from 0 to 59.</li> <li>– <i>hour</i>—Hour when a CRON timer event is triggered. Valid entries are numbers in the range from 0 to 23.</li> <li>– <i>day-of-month</i>—Day of the month when a CRON timer event is triggered. Valid entries are numbers in the range from 1 to 31.</li> <li>– <i>month</i>—Month when a CRON timer event is triggered. Valid entries are numbers in the range from 1 to 12 or the first three letters (not case-sensitive) of the name of the month.</li> <li>– <i>day-of-week</i>—Day of the week when a CRON timer event is triggered. Valid entries are numbers in the range from 0 to 6 (Sunday is 0) or the first three letters (not case-sensitive) of the name of the day.</li> </ul> </li> </ul> <p><b>Note</b> Ranges of numbers are allowed. The specified range is inclusive, and the two numbers are separated by a hyphen. For example, 8-11 after the hour field specifies execution of a CRON timer event at hours 8, 9, 10, and 11.</p> <p><b>Note</b> A field may contain an asterisk, *, which means that a field is not specified and can be any value.</p> <p><b>Note</b> Lists are permitted. A list is a set of numbers or ranges separated by a comma but no space. For example, 1,2,5,9 or 0-4,8-12.</p> <p><b>Note</b> Step values are permitted in conjunction with ranges. Following a range with <i>/number</i> specifies skips of the <i>number</i> value through the range. For example, 0-23/2 in the hour field specifies that an event is triggered every second hour. Steps are permitted after an asterisk, for example */2 means every two hours.</p> <p>Instead of the first five fields, some special strings can be entered. See the “Usage Guidelines” section for more details.</p>
<b>watchdog</b>	<p>Specifies that an event is triggered when the specified time counts down to zero. The timer automatically resets to the initial value and continues to count down.</p>
<b>name</b>	<p>(Optional) Specifies the name of the timer.</p> <ul style="list-style-type: none"> <li>• <i>timer-name</i>—Name of the timer.</li> </ul>

**Defaults**

No EEM events are triggered on the basis of time-specific events.

**Command Modes**

Applet configuration

**Command History**

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

**Usage Guidelines**

Instead of the five fields of a UNIX crontab entry as described in the syntax description table for the *cron-entry* argument, one of the following seven special strings can be entered:

- **@yearly**—An event is triggered once a year. This is the equivalent of specifying 0 0 1 1 \* for the first five fields.
- **@annually**—Same as **@yearly**.
- **@monthly**—An event is triggered once a month. This is the equivalent of specifying 0 0 1 \* \* for the first five fields.
- **@weekly**—An event is triggered once a week. This is the equivalent of specifying 0 0 \* \* 0 for the first five fields.
- **@daily**—An event is triggered once a day. This is the equivalent of specifying 0 0 \* \* \* for the first five fields.
- **@midnight**—Same as **@daily**.
- **@hourly**—An event is triggered once an hour. This is the equivalent of specifying 0 \* \* \* \* for the first five fields.

A CRON timer may not produce the intended result if the time-of-day clock is not set to the correct time. Network Time Protocol (NTP) services can be used to facilitate keeping an accurate time-of-day clock setting. For more details on NTP configuration, see the “Performing Basic System Management” chapter of the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*, Release 12.3.

**Examples**

The following example shows how to specify that an event is triggered one time after five hours:

```
Router(config)# event manager applet timer-absolute
Router(config-applet)# event timer absolute time 18000
```

The following example shows how to specify that an event is triggered once after six minutes and six milliseconds:

```
Router(config)# event manager applet timer-set
Router(config-applet)# event timer countdown time 360.006 name six-minutes
```

The following example shows how to specify that an event is triggered at 1:01 a.m. on January 1 each year:

```
Router(config)# event manager applet timer-cron1
Router(config-applet)# event timer cron cron-entry 1 1 1 1 * name Jan1
```

The following example shows how to specify that an event is triggered at noon on Monday through Friday of every week:

```
Router(config)# event manager applet timer-cron2
Router(config-applet)# event timer cron cron-entry 0 12 * * 1-5 name MonFri
```

The following example shows how to specify that an event is triggered at midnight on Sunday every week:

```
Router(config)# event manager applet timer-cron3
Router(config-applet)# event timer cron cron-entry @weekly name Sunday
```

The following example shows how to specify that an event is triggered every five hours:

```
Router(config)# event manager applet timer-watch
Router(config-applet)# event timer watchdog time 18000
```

---

**Related Commands**

Command	Description
<b>event manager applet</b>	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

---

# exception core-file

To specify the name of the core dump file, use the **exception core-file** command in global configuration mode. To return to the default core filename, use the **no** form of this command.

**exception core-file** *filename*

**no exception core-file**

Syntax Description	<i>filename</i>	Name of the core dump file saved on the server.
--------------------	-----------------	---

Defaults	The core file is named <i>hostname-core</i> , where <i>hostname</i> is the name of the router.
----------	--

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

Command History	Release	Modification
	10.2	This command was introduced.

Usage Guidelines	If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.
------------------	--



### Caution

Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

Examples	In the following example, the router is configured to use FTP to dump a core file named <code>dumpfile</code> to the FTP server at <code>172.17.92.2</code> when it crashes:
----------	--

```
Router(config)# ip ftp username red
Router(config)# ip ftp password blue
Router(config)# exception protocol ftp
Router(config)# exception dump 172.17.92.2
Router(config)# exception core-file dumpfile
```

Related Commands	Command	Description
	<b>exception dump</b>	Causes the router to dump a core file to a particular server when the router crashes.
	<b>exception memory</b>	Causes the router to create a core dump and reboot when certain memory size parameters are violated.

Command	Description
<b>exception protocol</b>	Configures the protocol used for core dumps.
<b>exception spurious-interrupt</b>	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
<b>ip ftp password</b>	Specifies the password to be used for FTP connections.
<b>ip ftp username</b>	Configures the username for FTP connections.

# exception crashinfo buffersize

To change the size of the buffer used for crashinfo files, use the **exception crashinfo buffersize** command in global configuration mode. To revert to the default buffer size, use the **no** form of this command.

**exception crashinfo buffersize** *kilobytes*

**no exception crashinfo buffersize** *kilobytes*

<b>Syntax Description</b>	<i>kilobytes</i>	Sets the size of the buffersize to the specified value within the range of 32 to 100 kilobytes. The default is 32KB.
---------------------------	------------------	--

<b>Defaults</b>	Crashinfo buffer is 32KB.
-----------------	---------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(4)T, 12.2(11)	This command was introduced for the Cisco 3600 series only (3620, 2640, and 3660 platforms).
	12.2(13)T	This command was implemented in 6400-NSP images.

<b>Usage Guidelines</b>	The crashinfo file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch writes the crash information to the console at the time of the failure, and the file is created the next time you boot the Cisco IOS image after the failure (instead of while the system is failing).
-------------------------	--

<b>Examples</b>	In the following example, the crashinfo buffer is set to 100 KB:
-----------------	--

```
Router(config)# exception crashinfo buffersize 100
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>exception crashinfo file</b>	Enables the creation of a diagnostic file at the time of unexpected system shutdowns.

# exception crashinfo dump

To specify the type of output information to be written to the crashinfo file, use the **exception crashinfo dump** command in global configuration mode. To remove this information from the crashinfo file, use the **no** form of this command.

**exception crashinfo dump** { **command** *cli* | **garbage-detector** }

**no exception crashinfo dump** { **command** *cli* | **garbage-detector** }

## Syntax Description

<b>command</b> <i>cli</i>	Indicates the Cisco IOS command for which you want the output information written to the crashinfo file.
<b>garbage-detector</b>	If a router crashes due to low memory, specifies that the output from the <b>show memory debug leaks summary</b> command should be written to the crashinfo file.

## Defaults

This command is disabled by default.

If a router crashes due to low memory, the output from the following Cisco IOS commands is written to the crashinfo file by default:

- **show process memory**
- **show processes cpu**
- **show memory summary**
- **show buffers**

If the **exception crashinfo dump garbage-detector** command is enabled, the output from the **show memory debug leaks summary** command is also written to the crashinfo file by default.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(11)T	This command was introduced.

## Usage Guidelines

A benefit for using the **exception crashinfo dump** command is that it allows users to customize the crashinfo file to contain information that is relevant to their troubleshooting situation.

## Examples

The following example shows how to specify that the output from the **show interfaces** command should be written to the crashinfo file:

```
exception crashinfo dump command show interfaces
```

---

**Related Commands**

Command	Description
<b>exception memory</b>	Sets free memory and memory block size threshold parameters.

# exception crashinfo file

To enable the creation of a diagnostic file at the time of unexpected system shutdowns, use the **exception crashinfo file** command in global configuration mode. To disable the creation of crashinfo files, use the **no** form of this command.

**exception crashinfo file** *device:filename*

**no exception crashinfo file** *device:filename*

## Syntax Description

<i>device:filename</i>	Specifies the flash device and file name to be used for storing the diagnostic information. The colon is required.
------------------------	--

## Defaults

Enabled

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(4)T, 12.2(11)	This command was introduced for the Cisco 3600 series only.
12.2(13)T	This command was implemented in 6400-NSP images.

## Usage Guidelines

The “crashinfo” file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch writes the crash information to the console at the time of the failure, and the file is created the next time you boot the IOS image after the failure (instead of while the system is failing). The filename will be *filename\_yyyymmdd-hhmmss*, where *y* is year, *m* is month, *d* is date, *h* is hour, and *s* is seconds.

## Examples

In the following example, a crashinfo file called “crashdata” will be created in the default flash memory device if a system crash occurs:

```
Router(config)# exception crashinfo file flash:crashinfo
```

## Related Commands

Command	Description
<b>exception crashinfo buffersize</b>	Changes the size of the crashinfo buffer.

# exception crashinfo maximum files

To enable a Cisco IOS device to automatically delete old crashinfo files to help create space for writing new crashinfo files when a system crashes, use the **exception crashinfo maximum files** command in global configuration mode. To disable automatic deletion of crashinfo files, use the **no** form of this command.

**exception crashinfo maximum files** *file-numbers*

**no exception crashinfo maximum files** *file-numbers*

<b>Syntax Description</b>	<i>file-numbers</i>	The number of most recent crashinfo files across all file systems in the device to be preserved when crashinfo files are being deleted automatically. The value ranges from 0 to 32.
---------------------------	---------------------	--

<b>Defaults</b>	This command is disabled by default.
-----------------	--------------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(11)T	This command was introduced.

<b>Usage Guidelines</b>	This command is effective only when a device crashes. If the value of the <i>file-number</i> argument is given as zero (0), none of the old crashinfo files will be preserved and all the old crashinfo files will be deleted across all file systems when the crashinfo files are being deleted automatically.
-------------------------	---

While booting a device, the default file is bootflash. If the file system does not have free space equivalent to or more than 250 KB, the system will display a warning. You can verify the available disk space and create free space for writing the crashinfo files.

<b>Examples</b>	The following example shows how to enable a Cisco IOS device this feature to automatically delete old crashinfo files to help create space for writing new crashinfo files when a system crashes. In this example, the device is configured to preserve the 22 most recent crashinfo files from previous crashinfo collections.
-----------------	---

```
Router(config)# exception crashinfo maximum files 22
```

Related Commands	Command	Description
	<b>exception crashinfo buffersize</b>	Changes the size of the crashinfo buffer.
	<b>exception crashinfo file</b>	Creates a diagnostic file at the time of unexpected system shutdown.

# exception dump

To configure the router to dump a core file to a particular server when the router crashes, use the **exception dump** command in global configuration mode. To disable core dumps, use the **no** form of this command.

**exception dump** *ip-address*

**no exception dump**

<b>Syntax Description</b>	<i>ip-address</i>	IP address of the server that stores the core dump file.
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.3	This command was introduced.

## Usage Guidelines



### Caution

Use the **exception dump** command only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

The core dump is written to a file named *hostname-core* on your server, where *hostname* is the name of the router. You can change the name of the core file by configuring the **exception core-file** command.

This procedure can fail for certain types of system crashes. However, if successful, the core dump file will be the size of the memory available on the processor (for example, 16 MB for a CSC/4).

## Examples

In the following example, a user configures a router to use FTP to dump a core file to the FTP server at 172.17.92.2 when it crashes:

```
Router(config)# ip ftp username red
Router(config)# ip ftp password blue
Router(config)# exception protocol ftp
Router(config)# exception dump 172.17.92.2
Router(config)# exception core-file dumpfile
```

Related Commands	Command	Description
	<b>exception core-file</b>	Specifies the name of the core dump file.
	<b>exception memory</b>	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
	<b>exception protocol</b>	Configures the protocol used for core dumps.
	<b>exception spurious-interrupt</b>	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
	<b>ip ftp password</b>	Specifies the password to be used for FTP connections.
	<b>ip ftp username</b>	Configures the username for FTP connections.
	<b>ip rcmd remote-username</b>	Configures the remote username to be used when requesting a remote copy using rcp.

# exception linecard

To enable storing of crash information for a line card and optionally specify the type and amount of information stored, use the **exception linecard** command in global configuration mode. To disable the storing of crash information for the line card, use the **no** form of this command.

```
exception linecard {all | slot slot-number} [corefile filename | main-memory size [k | m] |
queue-ram size [k | m] | rx-buffer size [k | m] | sqe-register-rx | sqe-register-tx | tx-buffer
size [k | m]]
```

```
no exception linecard
```

Syntax Description		
<b>all</b>		Stores crash information for all line cards.
<b>slot</b> <i>slot-number</i>		Stores crash information for the line card in the specified slot. Slot numbers range from 0 to 11 for the Cisco 12012 and 0 to 7 for the Cisco 12008 router.
<b>corefile</b> <i>filename</i>		(Optional) Stores the crash information in the specified file in NVRAM. The default filename is <i>hostname-core-slot-number</i> (for example, c12012-core-8).
<b>main-memory</b> <i>size</i>		(Optional) Stores the crash information for the main memory on the line card and specifies the size of the crash information. Size of the memory to store is 0 to 268435456.
<b>queue-ram</b> <i>size</i>		(Optional) Stores the crash information for the queue RAM memory on the line card and specifies the size of the crash information. Size of the memory to store can be from 0 to 1048576.
<b>rx-buffer</b> <i>size</i>		(Optional) Stores the crash information for the receive and transmit buffer on the line card and specifies the size of the crash information. Size of the memory to store can be from 0 to 67108864.
<b>tx-buffer</b> <i>size</i>		
<b>sqe-register-rx</b>		(Optional) Stores crash information for the receive or transmit silicon queuing engine registers on the line card.
<b>sqe-register-tx</b>		
<b>k</b>		(Optional) The <b>k</b> option multiplies the specified <i>size</i> by 1K (1024), and the <b>m</b> option multiplies the specified <i>size</i> by 1M (1024*1024).
<b>m</b>		

## Defaults

No crash information is stored for the line card.

If enabled with no options, the default is to store 256 MB of main memory.

## Command Modes

Global configuration

## Command History

Release	Modification
11.2 GS	This command was introduced for Cisco 12000 series Gigabit Switch Routers (GSRs).

---

**Usage Guidelines**

Use caution when enabling the **exception linecard** global configuration command. Enabling all options could cause a large amount (150 to 250 MB) of crash information to be sent to the server.

**Caution**

---

Use the **exception linecard** global configuration command only when directed by a technical support representative. Only enable options that the technical support representative requests you to enable. Technical support representatives need to be able to look at the crash information from the line card to troubleshoot serious problems on the line card. The crash information contains all the line card memory information including the main memory and transmit and receive buffer information.

---

---

**Examples**

In the following example, the user enables the storing of crash information for line card 8. By default, 256 MB of main memory is stored.

```
Router(config)# exception linecard slot 8
```

## exception memory

To set free memory and memory block size threshold parameters, use the **exception memory** command in global configuration mode. To disable this functionality, use the **no** form of this command.

```
exception memory { fragment [processor | io] size [interval 1] [reboot] | minimum [processor | io] size [reboot] }
```

```
no exception memory { fragment [processor | io] size [interval 1] [reboot] | minimum [processor | io] size [reboot] }
```

Syntax Description		
<b>fragment</b> <i>size</i>		Sets the minimum contiguous block of memory in the free pool, in bytes.
<b>processor</b>		(Optional) Specifies processor memory.
<b>io</b>		(Optional) Specifies I/O memory.
<b>interval 1</b>		(Optional) Checks the largest memory block size every 1 second. If the <b>interval 1</b> keyword is not configured, the memory block size is checked every 1 second by default.
<b>reboot</b>		(Optional) Reloads the router when a memory size threshold is violated. If the <b>reboot</b> keyword is not configured, the router will not reload when a memory size threshold is violated.
<b>minimum</b> <i>size</i>		Sets the minimum size of the free memory pool, in bytes.

**Defaults** This command is disabled by default.

**Command Modes** Global configuration

Command History	Release	Modification
	10.3	This command was introduced.
	12.3(11)T	The following keywords were added: <ul style="list-style-type: none"> <li>• <b>processor</b></li> <li>• <b>io</b></li> <li>• <b>interval 1</b></li> <li>• <b>reboot</b></li> </ul>

**Usage Guidelines** This command is used to troubleshoot memory leaks and memory fragmentation issues.

The free memory size is checked for every memory allocation. The largest memory block size is checked every 60 seconds by default. If the **interval 1** keyword is configured, the largest memory block size is checked every 1 second.

When a memory size threshold is violated, the router will display an error message and create a crashinfo file. A core dump file will also be created if the **exception dump** command is configured. The router will not reload unless the **reboot** keyword is configured.

**Caution**

Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

**Examples**

In the following example, the user configures the router to monitor the free memory. If the amount of free memory falls below 250,000 bytes, the router will create a crashinfo file and core dump file and reload.

```
Router(config)# exception dump 131.108.92.2
Router(config)# exception core-file memory.overrun
Router(config)# exception memory minimum 250000 reboot
```

**Related Commands**

Command	Description
<b>exception core-file</b>	Specifies the name of the core dump file.
<b>exception crashinfo dump</b>	Specifies the type of output information to be written to the crashinfo file.
<b>exception dump</b>	Configures the router to dump a core file to a particular server when the router crashes.
<b>exception protocol</b>	Configures the protocol used for core dumps.
<b>exception region-size</b>	Specifies the size of the region for the exception-time memory pool.
<b>ip ftp password</b>	Specifies the password to be used for FTP connections.
<b>ip ftp username</b>	Configures the username for FTP connections.

# exception memory ignore overflow

To configure the Cisco IOS software to correct corruption in memory block headers and allow a router to continue its normal operation, use the **exception memory ignore overflow** command in global configuration mode. To disable memory overflow correction, use the **no** form of this command.

```
exception memory ignore overflow {io | processor} [frequency time-gap] [maxcount corrections]
```

```
no exception memory ignore overflow {io | processor} [frequency time-gap] [maxcount corrections]
```

Syntax Description		
	<b>io</b>	Selects input/output (also called packet) memory.
	<b>processor</b>	Selects processor memory.
	<b>frequency</b> <i>time-gap</i>	(Optional) Specifies the minimum time gap between two memory block header corrections, in the range from 1 to 600 seconds. The default is once every 10 seconds.
	<b>maxcount</b> <i>corrections</i>	(Optional) Specifies the maximum number of memory block header corrections allowed, in the range from 1 to 1000. The default is 0, which sets an unlimited number of corrections.

**Defaults** The default is to allow the memory overflow correction once every 10 seconds, and for memory overflow corrections to happen an unlimited number of times.

**Command Modes** Global configuration

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

**Usage Guidelines** Use this command to improve device availability when software faults are detected in the network. You can configure the frequency and the maximum number of memory overflow corrections. If overflow correction is required more often than the configured value, a software forced reload is triggered because a severe system problem is indicated.

**Examples** The following example shows how to set a maximum of five processor memory block header corruption corrections to occur every 30 seconds:

```
exception memory ignore overflow processor frequency 30 maxcount 5
```

Related Commands

Command	Description
<b>show memory overflow</b>	Displays the details of a memory block header corruption correction.

# exception protocol

To configure the protocol used for core dumps, use the **exception protocol** command in global configuration mode. To configure the router to use the default protocol, use the **no** form of this command.

**exception protocol {ftp | rcp | tftp}**

**no exception protocol**

Syntax Description		
	<b>ftp</b>	Uses FTP for core dumps.
	<b>rcp</b>	Uses rcp for core dumps.
	<b>tftp</b>	Uses TFTP for core dumps. This is the default.

**Defaults** TFTP

**Command Modes** Global configuration

Command History	Release	Modification
	10.3	This command was introduced.

## Usage Guidelines



### Caution

Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

## Examples

In the following example, the user configures a router to use FTP to dump a core file to the FTP server at 172.17.92.2 when it crashes:

```
Router(config)# ip ftp username red
Router(config)# ip ftp password blue
Router(config)# exception protocol ftp
Router(config)# exception dump 172.17.92.2
```

Related Commands	Command	Description
	<b>exception core-file</b>	Specifies the name of the core dump file.
	<b>exception dump</b>	Causes the router to dump a core file to a particular server when the router crashes.
	<b>exception memory</b>	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
	<b>exception spurious-interrupt</b>	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
	<b>ip ftp password</b>	Specifies the password to be used for FTP connections.
	<b>ip ftp username</b>	Configures the username for FTP connections.

# exception region-size

To specify the size of the region for the exception-time memory pool, use the **exception region-size** command in global configuration mode. To use the default region size, use the **no** form of this command.

**exception region-size** *size*

**no exception region-size**

<b>Syntax Description</b>	<i>size</i>	The size of the region for the exception-time memory pool.
---------------------------	-------------	--

<b>Defaults</b>	16,384 bytes
-----------------	--------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.3	This command was introduced.

## Usage Guidelines



### Caution

Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

The **exception region-size** command is used to define a small amount of memory to serve as a fallback pool when the processor memory pool is marked corrupt. The **exception memory** command must be used to allocate memory to perform a core dump.

<b>Examples</b>	In the following example, the region size is set at 1024:
-----------------	---

```
Router(config)# exception region-size 1024
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>exception core-file</b>	Specifies the name of the core dump file.
	<b>exception dump</b>	Configures the router to dump a core file to a particular server when the router crashes.
	<b>exception memory</b>	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
	<b>exception protocol</b>	Configures the protocol used for core dumps.

Command	Description
<b>ip ftp password</b>	Specifies the password to be used for FTP connections.
<b>ip ftp username</b>	Configures the username for FTP connections.

# exception spurious-interrupt

To configure the router to create a core dump and reload after a specified number of spurious interrupts, use the **exception spurious-interrupt** command in global configuration mode. To disable the core dump and reload, use the **no** form of this command.

**exception spurious-interrupt** *number*

**no exception spurious-interrupt**

<b>Syntax Description</b>	<i>number</i>	(Optional) A number from 1 to 4294967295 that indicates the maximum number of spurious interrupts to include in the core dump before reloading.
---------------------------	---------------	---

<b>Defaults</b>	Disabled
-----------------	----------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.3	This command was introduced.

## Usage Guidelines



### Caution

Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core dump file to a server, the router will only dump the first 16 MB of the file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

## Examples

In the following example, the user configures a router to create a core dump with a limit of two spurious interrupts:

```
Router(config)# exception spurious-interrupt 2
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>exception core-file</b>	Specifies the name of the core dump file.
	<b>ip ftp password</b>	Specifies the password to be used for FTP connections.
	<b>ip ftp username</b>	Configures the user name for FTP connections.

# exec

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

**exec**

**no exec**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** The EXEC processes is enabled on all lines.

---

**Command Modes** Line configuration

---

Release	Modification
10.0	This command was introduced.

---



---

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

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

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

---

**Examples** The following example disables the EXEC process on line 7.

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

# exec-banner

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

**exec-banner**

**no exec-banner**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Enabled on all lines

**Command Modes** Line configuration

Release	Modification
10.0	This command was introduced.

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

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

The MOTD banners can also be disabled by the **no motd-banner** line configuration command, which disables MOTD banners on a line. If the **no exec-banner** command is configured on a line, the MOTD banner will be disabled regardless of whether the **motd-banner** command is enabled or disabled. [Table 30](#) summarizes the effects of the **exec-banner** command and the **motd-banner** command.

**Table 30** *Banners Displayed Based On exec-banner and motd-banner Combinations*

	<b>exec-banner</b> (default)	<b>no exec-banner</b>
<b>motd-banner</b> (default)	MOTD banner	None
	EXEC banner	
<b>no motd-banner</b>	EXEC banner	None

For reverse Telnet connections, the EXEC banner is never displayed. Instead, the incoming banner is displayed. The MOTD banner is displayed by default, but it is disabled if either the **no exec-banner** command or **no motd-banner** command is configured. [Table 31](#) summarizes the effects of the **exec-banner** command and the **motd-banner** command for reverse Telnet connections.

**Table 31** *Banners Displayed Based On exec-banner and motd-banner Combinations for Reverse Telnet Sessions to Async Lines*

	exec-banner (default)	no exec-banner
	MOTD banner	Incoming banner
<b>motd-banner</b> (default)	Incoming banner	
<b>no motd-banner</b>	Incoming banner	Incoming banner

### Examples

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

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

### Related Commands

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

# exec-character-bits

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

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

**no exec-character-bits**

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

**Defaults** 7-bit ASCII character set

**Command Modes** Line configuration

Command History	Release	Modification
	10.0	This command was introduced.

**Usage Guidelines** Setting the EXEC character width to 8 allows you to use special graphical and international characters in banners, prompts, and so on. However, setting the EXEC character width to 8 bits can cause failures. If a user on a terminal that is sending parity enters the **help** command, an “unrecognized command” message appears because the system is reading all 8 bits, and the eighth bit is not needed for the **help** command.



**Note**

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

**Examples**

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

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

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

# exec-timeout

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

**exec-timeout** *minutes* [*seconds*]

**no exec-timeout**

Syntax Description		
	<i>minutes</i>	Integer that specifies the number of minutes. The default is 10 minutes.
	<i>seconds</i>	(Optional) Additional time intervals in seconds.

Defaults	
	10 minutes

Command Modes	
	Line configuration

Command History	Release	Modification
	10.0	This command was introduced.

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

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

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

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

The following example sets a time interval of 10 seconds:

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

# execute-on

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

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

Syntax Description		
<b>slot</b> <i>slot-number</i>	Executes the command on the line card in the specified slot. Slot numbers can be chosen from the following ranges:	<ul style="list-style-type: none"> <li>• Cisco 12012 router: 0 to 11</li> <li>• Cisco 12008 access server: 0 to 7</li> <li>• Cisco AS5800 access server: 0 to 13</li> </ul>
<b>all</b>	Executes the command on all line cards.	
<b>master</b>	(AS5800 only) Executes the designated command on a Dial Shelf Controller (DSC). Do not use this option; it is used for technical support troubleshooting only.	
<i>command</i>	Cisco IOS command to remotely execute on the line card.	

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.2 GS	This command was introduced to support Cisco 12000 series Gigabit Switch Routers.
	11.3(2)AA	This command was implemented in images for the Cisco AS5800 series.

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

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



#### Tips

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

#### Cisco 12000 GSR Guidelines and Restrictions

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

**Timesaver**

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

**Cisco AS5800 Guidelines and Restrictions**

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

**Caution**

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

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

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

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

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

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

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

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

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

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

**Examples**

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

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

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

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

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

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

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

**Related Commands**

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

# exit (EXEC)

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

**exit**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	10.0	This command was introduced.

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

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

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

Related Commands	Command	Description
	<b>disconnect</b>	Disconnects a line.
	<b>end</b>	Ends your configuration session by exiting to EXEC mode.
	<b>exit (global)</b>	Exits from the current configuration mode to the next highest configuration mode.
	<b>logout</b>	Closes your connection to the device (equivalent to the <b>exit</b> command).

# exit (global)

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

**exit**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** All configuration modes

Command History	Release	Modification
	10.0	This command was introduced.

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

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

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

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

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

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

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

# file prompt

To specify the level of prompting, use the **file prompt** command in global configuration mode.

**file prompt [alert | noisy | quiet]**

Syntax Description	Parameter	Description
	<b>alert</b>	(Optional) Prompts only for destructive file operations. This is the default.
	<b>noisy</b>	(Optional) Confirms all file operation parameters.
	<b>quiet</b>	(Optional) Seldom prompts for file operations.

**Defaults** alert

**Command Modes** Global configuration

Command History	Release	Modification
	11.0	This command was introduced.

**Usage Guidelines** Use this command to change the amount of confirmation needed for different file operations. This command affects only prompts for confirmation of operations. The router will always prompt for missing information.

**Examples** The following example configures confirmation prompting for all file operations:

```
Router(config)# file prompt noisy
```

# file verify auto

To enable automatic image verification, use the **file verify auto** command in global configuration mode. To disable automatic image verification, use the **no** form of this command.

**file verify auto**

**no file verify auto**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Image verification is not automatically applied to all images that are copied or reloaded onto a router.

**Command Modes** Global configuration

Command History	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.

**Usage Guidelines** Image verification allows users to automatically verify the integrity of all Cisco IOS images. Thus, users can be sure that the image is protected from accidental corruption, which can occur at any time during transit, starting from the moment the files are generated by Cisco until they reach the user.

The **file verify auto** command enables image verification globally; that is, all images that are to be copied (via the **copy** command) or reloaded (via the **reload** command) are automatically verified. Although both the **copy** and **reload** commands have a **/verify** keyword that enables image verification, you must issue the keyword each time you want to copy or reload an image. The **file verify auto** command enables image verification by default so you no longer have to specify image verification multiple times.

If you have enabled image verification by default but prefer to disable verification for a specific image copy or reload, the **/noverify** keyword along with either the **copy** or the **reload** command will override the **file verify auto** command.

**Examples** The following example shows how to enable automatic image verification:

```
Router(config)# file verify auto
```

Related Commands	Command	Description
	<b>copy</b>	Copies any file from a source to a destination.
	<b>reload</b>	Reloads the operating system.

# filter-for-history

To define the type of information kept in the history table for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **filter-for-history** command in the appropriate submode of IP SLA monitor configuration or RTR configuration mode. To return to the default value, use the **no** form of this command.

**filter-for-history** { **none** | **all** | **overThreshold** | **failures** }

**no filter-for-history** { **none** | **all** | **overThreshold** | **failures** }

Syntax Description	none	No history kept. This is the default.
	<b>all</b>	All operations attempted are kept in the history table.
	<b>overThreshold</b>	Only packets that are over the threshold are kept in the history table.
	<b>failures</b>	Only packets that fail for any reason are kept in the history table.

**Defaults** No IP SLAs history is kept for an operation.

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

**Note**

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

**Command History**

Release	Modification
11.2	This command was introduced.

**Usage Guidelines**

Use the **filter-for-history** command to control what gets stored in the history table for an IP SLAs operation. To control how much history gets saved in the history table, use the **lives-of-history-kept**, **buckets-of-history-kept**, and the **samples-of-history-kept** commands.

**Note**

The **filter-for-history** command does not support the IP SLAs User Datagram Protocol (UDP) jitter operation.

An IP SLAs operation can collect history and capture statistics. By default, the history for an IP SLAs operation is not collected. If history is collected, each history bucket contains one or more history entries from the operation. When the operation type is ICMP path echo, an entry is created for each hop along the path that the operation takes to reach its destination. The type of entry stored in the history table is controlled by the **filter-for-history** command. The total number of entries stored in the history table is controlled by the combination of the **samples-of-history-kept**, **buckets-of-history-kept**, and **lives-of-history-kept** commands.

**Note**

Collecting history increases the RAM usage. Collect history only when you think there is a problem in the network.

**IP SLAs Operation Configuration Dependence on Cisco IOS Release**

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 32](#)). You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation.

The configuration mode for the **filter-for-history** command varies depending on the Cisco IOS release you are running (see [Table 32](#)) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the ICMP echo operation type is configured, you would enter the **filter-for-history** command in ICMP echo configuration mode (config-sla-monitor-echo) within IP SLA monitor configuration mode.

**Table 32** *Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release*

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

**Examples**

In the following examples, only operation packets that fail are kept in the history table. Note that the Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 32](#)).

**IP SLA Monitor Configuration**

```
ip sla monitor 1
  type echo protocol ipIcmpEcho 172.16.161.21
  lives-of-history-kept 1
  filter-for-history failures
!
ip sla monitor schedule 1 life forever start-time now
```

**RTR Configuration**

```
rtr 1
  type echo protocol ipIcmpEcho 172.16.161.21
  lives-of-history-kept 1
  filter-for-history failures
!
rtr schedule 1 life forever start-time now
```

**Related Commands**

Command	Description
<b>buckets-of-history-kept</b>	Sets the number of history buckets that are kept during the lifetime of the IP SLAs operation.
<b>ip sla monitor</b>	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
<b>lives-of-history-kept</b>	Sets the number of lives maintained in the history table for the IP SLAs operation.
<b>rtr</b>	Begins configuration for an IP SLAs operation and enters RTR configuration mode.
<b>samples-of-history-kept</b>	Sets the number of entries kept in the history table per bucket for the IP SLAs operation.

# format

To format a Class A, Class B, or Class C Flash file system, use the **format** command in EXEC mode.

## Class B and Class C Flash File Systems

**format** *filesystem1*:

## Class A Flash File System

**format** [**spare** *spare-number*] *filesystem1*: [[*filesystem2*:][*monlib-filename*]]



Caution

Reserve a certain number of memory sectors as spares, so that if some sectors fail, most of the Flash memory card can still be used. Otherwise, you must reformat the Flash card when some of the sectors fail.

### Syntax Description

<b>spare</b>	(Optional) Reserves spare sectors as specified by the <i>spare-number</i> argument when formatting Flash memory.
<i>spare-number</i>	(Optional) Number of the spare sectors to reserve on formatted Flash memory. Valid values are from 0 to 16. The default value is zero.
<i>filesystem1</i> :	Flash memory to format, followed by a colon.
<i>filesystem2</i> :	(Optional) File system containing the monlib file to use for formatting <i>filesystem1</i> followed by a colon.
<i>monlib-filename</i>	(Optional) Name of the ROM monitor library file (monlib file) to use for formatting the <i>filesystem1</i> argument. The default monlib file is the one bundled with the system software.  When used with HSA and you do not specify the <i>monlib-filename</i> argument, the system takes ROM monitor library file from the slave image bundle. If you specify the <i>monlib-filename</i> argument, the system assumes that the files reside on the slave devices.

### Command Default

None

### Command Modes

EXEC

### Command History

Release	Modification
11.0	This command was introduced.
12.3(14)T	Support for Class B Flash (USB Flash and USB eToken) File Systems was added.

**Usage Guidelines**

Use this command to format Class A, B, or C Flash memory file systems.

In some cases, you might need to insert a new PCMCIA Flash memory card and load images or backup configuration files onto it. Before you can use a new Flash memory card, you must format it.

Sectors in Flash memory cards can fail. Reserve certain Flash memory sectors as “spares” by using the optional *spare* argument on the **format** command to specify 0 to 16 sectors as spares. If you reserve a small number of spare sectors for emergencies, you can still use most of the Flash memory card. If you specify 0 spare sectors and some sectors fail, you must reformat the Flash memory card, thereby erasing all existing data.

The monlib file is the ROM monitor library. The ROM monitor uses this file to access files in the Flash file system. The Cisco IOS system software contains a monlib file.

In the command syntax, *filesystem1*: specifies the device to format and *filesystem2*: specifies the optional device containing the monlib file used to format *filesystem1*:. If you omit the optional *filesystem2*: and *monlib-filename* arguments, the system formats *filesystem1*: using the monlib file already bundled with the system software. If you omit only the optional *filesystem2*: argument, the system formats *filesystem1*: using the monlib file from the device you specified with the **cd** command. If you omit only the optional *monlib-filename* argument, the system formats *filesystem1*: using the *filesystem2*: monlib file. When you specify both arguments—*filesystem2*: and *monlib-filename*—the system formats *filesystem1*: using the monlib file from the specified device. You can specify *filesystem1*:’s own monlib file in this argument. If the system cannot find a monlib file, it terminates its formatting.

**Note**

You can read from or write to Flash memory cards formatted for Cisco 7000 series Route Processor (RP) cards in your Cisco 7200 and 7500 series routers, but you cannot boot the Cisco 7200 and 7500 series routers from a Flash memory card formatted for the Cisco 7000 series routers. Similarly, you can read from or write to Flash memory cards formatted for the Cisco 7200 and 7500 series routers in your Cisco 7000 series routers, but you cannot boot the Cisco 7000 series routers from a Flash memory card formatted for the Cisco 7200 and 7500 series routers.

**Examples**

The following example formats a Flash memory card inserted in slot 0:

```
Router# format slot0:

Running config file on this device, proceed? [confirm]y
All sectors will be erased, proceed? [confirm]y
Enter volume id (up to 31 characters): <Return>
Formatting sector 1 (erasing)
Format device slot0 completed
```

When the console returns to the EXEC prompt, the new Flash memory card is formatted and ready for use.

**Related Commands**

Command	Description
<b>cd</b>	Changes the default directory or file system.
<b>copy</b>	Copies any file from a source to a destination.
<b>delete</b>	Deletes a file on a Flash memory device.
<b>show file systems</b>	Lists available file systems.
<b>squeeze</b>	Permanently deletes Flash files by squeezing a Class A Flash file system.
<b>undelete</b>	Recovers a file marked “deleted” on a Class A or Class B Flash file system.

# format (bulkstat)

To specify the format to be used for the bulk statistics data file, use the format command in Bulk Statistics Transfer configuration mode. To disable a previously configured format specification and return to the default, use the **no** form of this command.

**format** { **bulkBinary** | **bulkASCII** | **schemaASCII** }

**no format** { **bulkBinary** | **bulkASCII** | **schemaASCII** }

## Syntax Description

bulkBinary	Binary format.
bulkASCII	ASCII (human-readable) format.
schemaASCII	ASCII format with additional bulk statistics schema tags.

## Defaults

The default bulk statistics transfer format is SchemaASCII.

## Command Modes

Bulk Statistics Transfer configuration (config-bulk-tr)

## Command History

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

## Usage Guidelines



### Note

In Cisco IOS Release 12.0(24)S, only the SchemaASCII format is supported. This command will not change the file format in this release.

The bulk statistics data file (VFile) contains two types of fields: tags and data. Tags are used to set-off data so as to distinguish portions (fields) of the file. All other information is in data fields.

For the BulkASCII and BulkBinary formats, data for a single data group (object list) can be collected more than once into the same bulk statistics data file (VFile) due to periodic polling. Each such instance of a data group can be treated as different “table” types.

Every object and table tag contains an additional sysUpTime field. Similarly each row tag contains the value of the sysUpTime when the data for that row was collected. This provides for a way to time-stamp the data.

For additional information on the structure of the bulk statistics data file formats, see the definitions in the CISCO-DATA-COLLECTION-MIB.

## Examples

In the following example, the bulk statistics data file is set to be SchemaASCII:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
Router(config-bulk-tr)# format schemaASCII
Router(config-bulk-tr)# exit
```

---

**Related Commands**

Command	Description
<b>snmp mib bulkstat transfer</b>	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.

---

# frequency (IP SLA)

To set the rate at which a specified IP Service Level Agreements (SLAs) operation repeats, use the **frequency** command in the appropriate submode of IP SLA monitor configuration or RTR configuration mode. To return to the default value, use the **no** form of this command.

**frequency** *seconds*

**no frequency**

---

## Syntax Description

*seconds*                      Number of seconds between the IP SLAs operations.

---



---

## Defaults

60 seconds

---

## Command Modes

### IP SLA Monitor Configuration

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

### RTR Configuration

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



### Note

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

---

**Command History**

Release	Modification
11.2	This command was introduced.

**Usage Guidelines**

A single IP SLAs operation will repeat at a given frequency for the lifetime of the operation. For example, a User Datagram Protocol (UDP) jitter operation with a frequency of 60 sends a collection of data packets (simulated network traffic) once every 60 seconds, for the lifetime of the operation. The default simulated traffic for a UDP jitter operation consists of ten packets sent 20 milliseconds apart. This “payload” is sent when the operation is started, then is sent again 60 seconds later.

If an individual IP SLAs operation takes longer to execute than the specified **frequency** value, a statistics counter called “busy” is incremented rather than immediately repeating the operation.

The value specified for the **frequency** command cannot be less than the value specified for the **timeout** command.

**Note**

We recommend that you do not set the frequency value to less than 60 seconds because the potential overhead from numerous active operations could significantly affect network performance.

**IP SLAs Operation Configuration Dependence on Cisco IOS Release**

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 33](#)). You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation.

The configuration mode for the **frequency** command varies depending on the Cisco IOS release you are running (see [Table 33](#)) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the ICMP echo operation type is configured, you would enter the **frequency** command in ICMP echo configuration mode (config-sla-monitor-echo) within IP SLA monitor configuration mode.

**Table 33** *Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release*

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

**Examples**

The following examples show how to configure an IP SLAs ICMP echo operation (operation 10) to repeat every 90 seconds. Note that the Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 33](#)).

**IP SLA Monitor Configuration**

```
ip sla monitor 10
  type echo protocol ipIcmpEcho 172.16.1.175
  frequency 90
!
ip sla monitor schedule 10 life 300 start-time after 00:05:00
```

**RTR Configuration**

```
rtr 10
  type echo protocol ipIcmpEcho 172.16.1.175
  frequency 90
!
rtr schedule 10 life 300 start-time after 00:05:00
```

**Related Commands**

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

# fsck

To check a File Allocation Table (FAT)-based disk or Class C filesystem for damage and to repair any problems, use the **fsck** command in privileged EXEC mode.

**fsck** [/nocrc] filesystem: [/automatic]

Syntax Description		
	<b>/nocrc</b>	(Optional. This keyword is available for Class C Flash file systems only.) Omits cyclic redundancy checks (CRCs).
	<i>filesystem:</i>	The filesystem prefix indicating the disk to be checked. The colon (:) is required. Typically, the filesystem prefix will be <b>disk0:</b> or <b>disk1:</b> .
	<b>/automatic</b>	(Optional. This keyword is available for ATA FAT-based disks only.) Specifies that the check and repair actions should proceed automatically. This option can be used to skip the prompts for each check and repair action.

**Defaults** If the **/automatic** keyword is not used, CLI prompts for actions are issued.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.3 AA	This command was introduced.
	12.2(13)T, 12.0(22)S	This command was implemented on the Cisco 7000 family of routers and on the Cisco 10000 and 12000 series to support ATA disks.

**Usage Guidelines** This command will perform all of the steps necessary to remove corrupted files and reclaim unused disk space. Changes include checking for incorrect file sizes, cluster loops, and so on. The default form of this command will issue multiple prompts to confirm each of the changes. However, you can skip these prompts by using the **/automatic** keyword when issuing the command.

When the **/automatic** keyword is used you will be prompted to confirm that you want the automatic option. Prompts for actions will be skipped, but all actions performed will be displayed to the terminal (see the example below).

This command works with ATA PCMCIA cards formatted in DOS, or for Class C Flash file systems.



**Note**

Only one partition (the active partition) will be checked in the ATA disk.

**Examples** The following example shows sample output from using the **fsck** command in automatic mode:

```
Router# fsck /automatic disk1:
Proceed with the automatic mode? [yes] y
Checking the boot sector and partition table...
Checking FAT, Files and Directories...
```

```
Start cluster of file disk1:/file1 is invalid, removing file
File disk1:/file2 has a free/bad cluster, truncating...
File disk1:/file2 truncated.
File disk1:/file3 has a free/bad cluster, truncating...
File disk1:/file3 truncated.
File disk1:/file4 has a invalid cluster, truncating...
File disk1:/file4 truncated.
File disk1:/file5 has a invalid cluster, truncating...
File disk1:/file5 truncated.
File disk1:/file6 has a invalid cluster, truncating...
File disk1:/file6 truncated.
File size of disk1:/file7 is not correct, correcting it
File disk1:/file8 cluster chain has a loop, truncating it
File disk1:/file8 truncated.
File disk1:/file9 cluster chain has a loop, truncating it
File disk1:/file9 truncated.
File disk1:/file16 has a free/bad cluster, truncating...
File disk1:/file16 truncated.
File disk1:/file20 has a free/bad cluster, truncating...
File disk1:/file20 truncated.
Reclaiming unused space...
Created file disk1:/fsck-4 for an unused cluster chain
Created file disk1:/fsck-41 for an unused cluster chain
Created file disk1:/fsck-73 for an unused cluster chain
Created file disk1:/fsck-106 for an unused cluster chain
Created file disk1:/fsck-121 for an unused cluster chain
Created file disk1:/fsck-132 for an unused cluster chain
Created file disk1:/fsck-140 for an unused cluster chain
Created file disk1:/fsck-156 for an unused cluster chain
Created file disk1:/fsck-171 for an unused cluster chain
Created file disk1:/fsck-186 for an unused cluster chain
Created file disk1:/fsck-196 for an unused cluster chain
Created file disk1:/fsck-235 for an unused cluster chain
Created file disk1:/fsck-239 for an unused cluster chain
Updating FAT...
fsck of disk1: complete
```

# full-help

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

## full-help

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Disabled

---

**Command Modes** Line configuration

---

Command History	Release	Modification
	10.0	This command was introduced.

---



---

**Usage Guidelines** The **full-help** command enables (or disables) an unprivileged user to see all of the help messages available. It is used with the **show ?** command.

---

**Examples** In the following example, the **show ?** command is used first with full-help disabled. Then **full-help** is enabled for the line, and the **show ?** command is used again to demonstrate the additional help output that is displayed.

```
Router> show ?

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

Router> enable
Password:<letmein>

Router# configure terminal
```

```

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# line console 0
Router(config-line)# full-help
Router(config-line)# exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router# disable
Router> show ?

  access-expression  List access expression
  access-lists       List access lists
  aliases             Display alias commands
  apollo              Apollo network information
  appletalk           AppleTalk information
  arp                 ARP table
  async               Information on terminal lines used as router interfaces
  bootflash           Boot Flash information
  bridge              Bridge Forwarding/Filtering Database [verbose]
  bsc                 BSC interface information
  bstun               BSTUN interface information
  buffers             Buffer pool statistics
  calendar            Display the hardware calendar
  .
  .
  .
  translate           Protocol translation information
  ttycap              Terminal capability tables
  users               Display information about terminal lines
  version             System hardware and software status
  vines               VINES information
  vlans               Virtual LANs Information
  whoami              Info on current tty line
  x25                 X.25 information
  xns                 XNS information
  xremote             XRemote statistics

```

**Related Commands**

Command	Description
<b>help</b>	Displays a brief description of the help system.

# help

To display a brief description of the help system, use the **help** command in any command mode.

## help

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** User EXEC  
Privileged EXEC  
All configuration modes

---

Command History	Release	Modification
	10.0	This command was introduced.

---



---

**Usage Guidelines** The **help** command provides a brief description of the context-sensitive help system, which functions as follows:

- To list all commands available for a particular command mode, enter a question mark (?) at the system prompt.
- To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by a question mark (?). This form of help is called *word help*, because it lists only the keywords or arguments that begin with the abbreviation you entered.
- To list the keywords and arguments associated with a command, enter a question mark (?) in place of a keyword or argument on the command line. This form of help is called *command syntax help*, because it lists the keywords or arguments that apply based on the command, keywords, and arguments you have already entered.

---

**Examples** In the following example, the **help** command is used to display a brief description of the help system:

```
Router# help
```

```
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
```

```
Two styles of help are provided:
```

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

The following example shows how to use word help to display all the privileged EXEC commands that begin with the letters “co.” The letters entered before the question mark are reprinted on the next command line to allow the user to continue entering the command.

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

The following example shows how to use command syntax help to display the next argument of a partially complete **access-list** command. One option is to add a wildcard mask. The <cr> symbol indicates that the other option is to press Enter to execute the command without adding any more keywords or arguments. The characters entered before the question mark are reprinted on the next command line to allow the user to continue entering the command or to execute that command as it is.

```
Router(config)# access-list 99 deny 131.108.134.234 ?
A.B.C.D Mask of bits to ignore
<cr>
Router(config)# access-list 99 deny 131.108.134.234
```

**Related Commands**

Command	Description
<b>full-help</b>	Enables help for the full set of user-level commands for a line.

# hidekeys

To suppress the display of password information in configuration log files, use the **hidekeys** command in configuration change logger configuration mode. To allow the display of password information in configuration log files, use the **no** form of this command.

**hidekeys**

**no hidekeys**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Password information is displayed.

**Command Modes** Configuration change logger configuration

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.

**Usage Guidelines** Enabling the **hidekeys** command increases security by preventing password information from being displayed in configuration log files.

**Examples** The following example shows how to prevent password information from being displayed in configuration log files:

```
Router(config-archive-log-config)# hidekeys
```

Related Commands	Command	Description
	<b>archive</b>	Enters archive configuration mode.
	<b>log config</b>	Enters configuration change logger configuration mode.
	<b>logging enable</b>	Enables the logging of configuration changes.
	<b>logging size</b>	Specifies the maximum number of entries retained in the configuration log.
	<b>notify syslog</b>	Enables the sending of notifications of configuration changes to a remote syslog.
	<b>show archive log config</b>	Displays entries from the configuration log.

# history

To enable the command history function, use the **history** command in line configuration mode. To disable the command history function, use the **no** form of this command.

**history**

**no history**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Enabled with ten command lines in the buffer.

**Command Modes** Line configuration

Command History	Release	Modification
	10.0	This command was introduced.

**Usage Guidelines**

The command history function provides a record of EXEC commands that you have entered. This function is particularly useful for recalling long or complex commands or entries, including access lists.

To change the number of command lines that the system will record in its history buffer, use the **history size** line configuration command.

The **history** command enables the history function with the last buffer size specified or, if there was not a prior setting, with the default of ten lines. The **no history** command disables the history function.

The **show history** EXEC command will list the commands you have entered, but you can also use your keyboard to display individual commands. [Table 34](#) lists the keys you can use to recall commands from the command history buffer.

**Table 34 History Keys**

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

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

---

**Examples**

In the following example, the command history function is disabled on line 4:

```
Router(config)# line 4
Router(config-line)# no history
```

---

**Related Commands**

Command	Description
<b>history size</b>	Sets the command history buffer size for a particular line.
<b>show history</b>	Lists the commands you have entered in the current EXEC session.
<b>terminal history</b>	Enables the command history function for the current terminal session or changes the size of the command history buffer for the current terminal session.

# history size

To change the command history buffer size for a particular line, use the **history size** command in line configuration mode. To reset the command history buffer size to ten lines, use the **no** form of this command.

**history size** *number-of-lines*

**no history size**

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

<b>Defaults</b>	10 command lines
-----------------	------------------

<b>Command Modes</b>	Line configuration
----------------------	--------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

**Usage Guidelines** The **history size** command should be used in conjunction with the **history** and **show history** commands. The **history** command enables or disables the command history function. The **show history** command lists the commands you have entered in the current EXEC session. The number of commands that the history buffer will show is set by the **history size** command.



**Note**

The **history size** command only sets the size of the buffer; it does not reenables the history function. If the **no history** command is used, the **history** command must be used to reenables this function.

**Examples** The following example displays line 4 configured with a history buffer size of 35 lines:

```
Router(config)# line 4
Router(config-line)# history size 35
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>history</b>	Enables or disables the command history function.
	<b>show history</b>	Lists the commands you have entered in the current EXEC session.
	<b>terminal history size</b>	Enables the command history function for the current terminal session or changes the size of the command history buffer for the current terminal session.

# hold-character

To define the local hold character used to pause output to the terminal screen, use the **hold-character** command in line configuration mode. To restore the default, use the **no** form of this command.

**hold-character** *ascii-number*

**no hold-character**

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

<b>Defaults</b>	No hold character is defined.
-----------------	-------------------------------

<b>Command Modes</b>	Line configuration
----------------------	--------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

<b>Usage Guidelines</b>	The Break character is represented by zero; NULL cannot be represented. To continue the output, enter any character after the hold character. To use the hold character in normal communications, precede it with the escape character. See the “ASCII Character Set” appendix for a list of ASCII characters.
-------------------------	--

<b>Examples</b>	The following example sets the hold character to Ctrl-S, which is ASCII decimal character 19:
-----------------	---

```
Router(config)# line 8
Router(config-line)# hold-character 19
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>terminal hold-character</b>	Sets or changes the hold character for the current session.

# hops-of-statistics-kept

To set the number of hops for which statistics are maintained per path for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **hops-of-statistics-kept** command in the appropriate submode of IP SLA monitor configuration or RTR configuration mode. To return to the default value, use the **no** form of this command.

**hops-of-statistics-kept** *size*

**no hops-of-statistics-kept**

<b>Syntax Description</b>	<i>size</i>	Number of hops for which statistics are maintained per path.
---------------------------	-------------	--

<b>Defaults</b>	16 hops
-----------------	---------

<b>Command Modes</b>	<p><b>IP SLA Monitor Configuration</b></p> <p>ICMP path echo configuration (config-sla-monitor-pathEcho)</p> <p><b>RTR Configuration</b></p> <p>ICMP path echo configuration (config-rtr-pathEcho)</p>
----------------------	--



**Note**

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.2	This command was introduced.

<b>Usage Guidelines</b>	When the number of hops reaches the size specified, no further hop-based information is stored.
-------------------------	---



**Note**

This command is supported by the IP SLAs ICMP path echo operation only.

### IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 35](#)). You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation.

The configuration mode for the **hops-of-statistics-kept** command varies depending on the Cisco IOS release you are running (see [Table 35](#)) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the ICMP path echo operation type is configured, you would enter the **hops-of-statistics-kept** command in ICMP path echo configuration mode (config-sla-monitor-pathEcho) within IP SLA monitor configuration mode.

**Table 35** Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release

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

## Examples

The following examples show how to monitor the statistics of IP SLAs ICMP path echo operation 2 for ten hops only. Note that the Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 35](#)).

### IP SLA Monitor Configuration

```
ip sla monitor 2
  type pathecho protocol ipIcmpEcho 172.16.1.177
  hops-of-statistics-kept 10
!
ip sla monitor schedule 2 life forever start-time now
```

### RTR Configuration

```
rtr 2
  type pathecho protocol ipIcmpEcho 172.16.1.177
  hops-of-statistics-kept 10
!
rtr schedule 2 life forever start-time now
```

## Related Commands

Command	Description
<b>distributions-of-statistics-kept</b>	Sets the number of statistics distributions kept per hop during the lifetime of the IP SLAs operation.
<b>hours-of-statistics-kept</b>	Sets the number of hours for which statistics are maintained for the IP SLAs operation.
<b>ip sla monitor</b>	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
<b>paths-of-statistics-kept</b>	Sets the number of paths for which statistics are maintained per hour for the IP SLAs operation.
<b>rtr</b>	Begins configuration for an IP SLAs operation and enters RTR configuration mode.
<b>statistics-distribution-interval</b>	Sets the time interval for each statistics distribution kept for the IP SLAs operation.

# hostname

To specify or modify the host name for the network server, use the **hostname** command in global configuration mode.

**hostname** *name*

Syntax Description	<i>name</i>	New host name for the network server.
--------------------	-------------	---------------------------------------

Defaults	The default host name is Router.
----------	----------------------------------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	The host name is used in prompts and default configuration filenames.
------------------	---

Do not expect case to be preserved. Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, *Choosing a Name for Your Computer*.

The name must also follow the rules for ARPANET host names. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names must be 63 characters or fewer. A host name of less than 10 characters is recommended. For more information, refer to RFC 1035, *Domain Names—Implementation and Specification*.

On most systems, a field of 30 characters is used for the host name and the prompt in the CLI. Note that the length of your host name may cause longer configuration mode prompts to be truncated. For example, the full prompt for service profile configuration mode is:

```
(config-service-profile)#
```

However, if you are using the host-name of "Router", you will only see the following prompt (on most systems):

```
Router(config-service-profil)#
```

If the hostname is longer, you will see even less of the prompt:

```
Basement-rtr2(config-service)#
```

Keep this behavior in mind when assigning a name to your system (using the **hostname** global configuration command). If you expect that users will be relying on mode prompts as a CLI navigation aid, you should assign host names of no more than nine characters.

---

**Examples**

The following example changes the host name to “sandbox”:

```
Router(config)# hostname sandbox
sandbox(config)#
```

---

**Related Commands**

Command	Description
<b>setup</b>	Enables you to make major changes to your configurations, for example, adding a protocol suit, making major addressing scheme changes, or configuring newly installed interfaces.

# hours-of-statistics-kept

To set the number of hours for which statistics are maintained for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **hours-of-statistics-kept** command in the appropriate submode of IP SLA monitor configuration or RTR configuration mode. To return to the default value, use the **no** form of this command.

**hours-of-statistics-kept** *hours*

**no hours-of-statistics-kept**

Syntax Description	<i>hours</i>	Number of hours that statistics are maintained. The default is 2 hours.
--------------------	--------------	---

Defaults	2 hours
----------	---------

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



#### Note

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

**Command History**

Release	Modification
11.2	This command was introduced.

**Usage Guidelines**

When the number of hours exceeds the specified value, the statistics table wraps (that is, the oldest information is replaced by newer information).

**IP SLAs Operation Configuration Dependence on Cisco IOS Release**

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 36](#)). You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation.

The configuration mode for the **hours-of-statistics-kept** command varies depending on the Cisco IOS release you are running (see [Table 36](#)) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the ICMP echo operation type is configured, you would enter the **hours-of-statistics-kept** command in ICMP echo configuration mode (config-sla-monitor-echo) within IP SLA monitor configuration mode.

**Table 36** *Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release*

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

**Examples**

The following examples show how to maintain 3 hours of statistics for IP SLAs ICMP path echo operation 2. Note that the Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 36](#)).

**IP SLA Monitor Configuration**

```
ip sla monitor 2
  type pathecho protocol ipIcmpEcho 172.16.1.177
  hours-of-statistics-kept 3
!
ip sla monitor schedule 2 life forever start-time now
```

**RTR Configuration**

```
rtr 2
  type pathecho protocol ipIcmpEcho 172.16.1.177
  hours-of-statistics-kept 3
!
rtr schedule 2 life forever start-time now
```

**Related Commands**

Command	Description
<b>distributions-of-statistics-kept</b>	Sets the number of statistics distributions kept per hop during the lifetime of the IP SLAs operation.
<b>hops-of-statistics-kept</b>	Sets the number of hops for which statistics are maintained per path for the IP SLAs operation.
<b>ip sla monitor</b>	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
<b>paths-of-statistics-kept</b>	Sets the number of paths for which statistics are maintained per hour for the IP SLAs operation.
<b>rtr</b>	Begins configuration for an IP SLAs operation and enters RTR configuration mode.
<b>statistics-distribution-interval</b>	Sets the time interval for each statistics distribution kept for the IP SLAs operation.

# http-raw-request

To explicitly specify the options for a GET request for a Cisco IOS IP Service Level Agreements (SLAs) Hypertext Transfer Protocol (HTTP) operation, use the **http-raw-request** command in the appropriate submode of IP SLA monitor configuration or RTR configuration mode.

## http-raw-request

**Syntax Description** This command has no arguments or keywords.

**Defaults** No options are specified for a GET request.

**Command Modes** IP SLA Monitor Configuration  
HTTP configuration (config-sla-monitor-http)

RTR Configuration  
HTTP configuration (config-rtr-http)



**Note**

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

Command History	Release	Modification
	12.0(5)T	This command was introduced.

**Usage Guidelines** Use the **http-raw-request** command to explicitly specify the content of an HTTP request. Use HTTP version 1.0 commands after entering the **http-raw-request** command.

IP SLAs will specify the content of an HTTP request if you use the **type http operation get** command. IP SLAs will send the HTTP request, receive the reply, and report round-trip time (RTT) statistics (including the size of the page returned).

### IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 37](#)). You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation.

The configuration mode for the **http-raw-request** command varies depending on the Cisco IOS release you are running (see [Table 37](#)) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the HTTP operation type is configured, you would enter the **http-raw-request** command in HTTP configuration mode (config-sla-monitor-http) within IP SLA monitor configuration mode.

**Table 37** Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release

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

**Examples**

In the following examples, IP SLAs operation 6 is created and configured as an HTTP operation. The HTTP **GET** command is explicitly specified. Note that the Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 37](#)).

**IP SLA Monitor Configuration**

```
ip sla monitor 6
 type http operation raw url http://www.cisco.com
 http-raw-request
 GET /index.html HTTP/1.0\r\n
 \r\n
 !
 ip sla monitor schedule 6 start-time now
```

**RTR Configuration**

```
rtr 6
 type http operation raw url http://www.cisco.com
 http-raw-request
 GET /index.html HTTP/1.0\r\n
 \r\n
 !
 rtr schedule 6 start-time now
```

**Related Commands**

Command	Description
<b>ip sla monitor</b>	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
<b>rtr</b>	Begins configuration for an IP SLAs operation and enters RTR configuration mode.
<b>type http operation</b>	Configures an HTTP IP SLAs operation.

# insecure

To configure a line as insecure, use the **insecure** command in line configuration mode. To disable this function, use the **no** form of this command.

**insecure**

**no insecure**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Disabled

---

**Command Modes** Line configuration

---

Release	Modification
10.0	This command was introduced.

---



---

**Usage Guidelines** Use this command to identify a modem line as insecure for DEC local area transport (LAT) classification.

---

**Examples** In the following example, line 10 is configured as an insecure dialup line:

```
Router(config)# line 10
Router(config-line)# insecure
```

# instance

To configure the MIB object instances to be used in a bulk statistics schema, use the **instance** command in Bulk Statistics Schema configuration mode. To remove an SNMP bulk statistics object list, use the **no** form of this command.

```
instance { exact | wild } { interface interface-id [sub-if] | controller controller-id [sub-if] | oid
OID }
```

```
no instance { exact | wild } { interface interface-id [sub-if] | controller controller-id [sub-if] | oid
OID }
```

## Syntax Description

<b>exact</b>	Indicates that the specified instance (interface, controller, or OID), when appended to the object list, is the complete OID to be used in this schema.
<b>wild</b>	Indicates that all instances that fall within the specified interface, controller, or OID range should be included in this schema.
<b>interface</b> <i>interface-id</i>	Specifies a specific interface or group of interfaces for the schema. Allows you to specify the IfIndex object instances for this interface instead of entering the OID. To display the list of available interfaces, use the <b>instance exact interface ?</b> command.
<b>controller</b> <i>controller-id</i>	Specifies a specific controller or group of controllers for the schema. Allows you to specify the IfIndex object instances for the interfaces on this controller instead of entering the OID. To display the list of available controllers, use the <b>instance exact controller ?</b> command.
<b>sub-if</b>	(Optional) Specifies that the object instances should be polled for all subinterfaces of the specified interface or controller in addition to the object instances for the main interface.
<b>oid</b> <i>OID</i>	The object identifier (OID) that, when appended to the object list, specifies the complete (or wildcarded) OID for the objects to be monitored.

## Defaults

If the **sub-if** keyword is not used, the subinterfaces of the interface or controller will not be polled.

## Command Modes

Bulk Statistics Schema configuration (config-bulk-sc)

## Command History

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

## Usage Guidelines

The **instance** command specifies the instance information for objects in the schema being configured. The specific instances of MIB objects for which data should be collected are determined by appending the value of the **instance** command to the objects specified in the associated object list. In other words, the schema **object-list** when combined with the schema **instance** specifies a complete MIB object identifier (OID).

The **instance exact** command indicates that the specified instance, when appended to the object list, is the complete OID.

The **instance wild** command indicates that all subindices of the specified OID belong to this schema. In other words, the **wild** keyword allows you to specify a partial, “wild carded” instance.

Instead of specifying an OID, you can specify a specific interface. The **interface interface-id** keyword and argument allow you to specify an interface name and number (for example, Ethernet 0) instead of specifying the ifIndex OID for the interface. Similarly, the **controller controller-id** syntax allows you to specify a controller interface.

The optional **sub-if** keyword, when added after specifying an interface or controller, includes the ifIndexes for all sub-interfaces of the interface you specified.

Only one **instance** command can be configured per schema.

## Examples

In the following example, the user configures the router to collect bulk statistics for the ifInOctets object (from the IF-MIB) for the Ethernet interface 3/0. In this example, 3 is the ifIndex instance for interface Ethernet3/0. The instance (3) when combined with the object list (ifIndex; 1.3.6.1.2.1.2.2.1.1) translates to the OID 1.3.6.1.2.1.2.2.1.1.3.

```
Router# configure terminal
Router(config)# snmp mib bulkstat object-list EOInOctets
! The following command specifies the object 1.3.6.1.2.1.2.2.1.1.3 (ifIndex)
Router(config-bulk-objects)# add ifIndex
Router(config-bulk-objects)# exit
Router(config)# snmp mib bulkstat schema E0
Router(config-bulk-sc)# object-list EOInOctets
! The following command is equivalent to "instance exact oid 3".
Router(config-bulk-sc)# instance exact interface Ethernet 3/0
Router(config-bulk-sc)# exit
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema E0
Router(config-bulk-tr)# url primary ftp://user:password@host/ftp/user/bulkstat1
Router(config-bulk-tr)# url secondary tftp://user@host/tftp/user/bulkstat1
Router(config-bulk-tr)# format schemaASCII
Router(config-bulk-tr)# transfer-interval 30
Router(config-bulk-tr)# retry 5
Router(config-bulk-tr)# enable
Router(config-bulk-tr)# exit
Router(config)# do copy running-config startup-config
```

## Related Commands

Command	Description
<b>object-list</b>	Configures the bulk statistics object list to be used in the bulk statistics schema.
<b>snmp mib bulkstat schema</b>	Names an SNMP bulk statistics schema and enters Bulk Statistics Schema configuration mode.

# instance (resource group)

To add RUs to a specified resource group, use the **instance** command in resource group configuration mode. To disable this function, use the **no** form of this command.

**instance** *instance-name*

**no instance** *instance-name*

<b>Syntax Description</b>	<i>instance-name</i>	Name of the RU you want to add to the resource group (for example, <b>http</b> , <b>snmp</b> , and so on).
---------------------------	----------------------	--

<b>Command Default</b>	Disabled
------------------------	----------

<b>Command Modes</b>	Resource group configuration
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(14)T	This command was introduced.

**Usage Guidelines**

Before adding RUs to a resource group, you must create a resource group using the **user group resource-group-name type resource-user-type** command in ERM configuration mode.

For example, say you have created a resource group with the name lowPrioUsers and iosprocess as the type. You have some low-priority RUs or tasks like HTTP and SNMP, and you want to set a threshold for all the low-priority RUs together, not separately. You must add the RUs to the resource group using the **instance instance-name** command and then apply a resource policy. If the resource policy you applied sets a minor rising threshold value of 10% for the resource group, then when the accumulated usage of both HTTP and SNMP RUs crosses 10%, a notification is sent to the RUs in the resource group lowPrioUsers. That is, if HTTP usage is 4% and SNMP usage is 7%, then a notification is sent to the resource group. This facility helps to set thresholds for a group of RUs, as it is difficult to set thresholds for every single RU individually.

**Examples**

The following example shows how to add HTTP RU to a resource group named lowPrioUsers:

```
Router(config-erm)# user group lowPrioUsers type iosprocess
Router(config-res-group)# instance http
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>policy (resource group)</b>	Applies a policy to all the RUs in the resource group.
	<b>user (ERM)</b>	Creates a resource group.

# international

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

**international**

**no international**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Disabled

**Command Modes** Line configuration

Release	Modification
11.3	This command was introduced.

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

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

```
line vty 4
  international
```

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

# ip address dynamic

To discover a customer premises equipment (CPE) router's IP address dynamically based on an aggregator router's IP address, use the **ip address dynamic** command in Frame Relay DLCI interface configuration mode. To disable this request, use the **no** form of this command.

**ip address dynamic**

**no ip address dynamic**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No IP address discovery request is made.

**Command Modes** Frame Relay DLCI interface configuration

## Command History

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

## Usage Guidelines

When you enter the **ip address dynamic** command, the CPE router sends an Inverse Address Resolution Protocol (ARP) request to the aggregator router asking for the IP address of its interface. The aggregator router replies with its own subinterface's IP address. The CPE router then calculates a valid IP address and a suitable netmask for its subinterface based on the data received from the aggregator router. The aggregator router is polled at regular intervals. If the IP address on the aggregator router's interface changes, the CPE router's IP address will adjust as necessary.

You can check the assigned IP address by entering the **show interface** command and specifying the subinterface being configured.



### Note

The **ip address dynamic** command is only applicable for Frame Relay point-to-point subinterfaces.

## Examples

The following example shows how to configure serial interface 1 to run Frame Relay. Its subinterface is then configured to discover the IP address using the **ip address dynamic** command.

```
interface Serial 1
  encapsulation frame
interface serial 1.1 point-to-point
  frame-relay interface-dlci 100
  ip address dynamic
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>frame-relay interface-dlci</b>	Assigns a data link connection identifier (DLCI) to a specified Frame Relay subinterface on the router or access server, and enters Frame Relay DLCI interface configuration mode.

# ip bootp server

To enable the Bootstrap Protocol (BOOTP) service on your routing device, use the **ip bootp server** command in global configuration mode. To disable BOOTP services, use the **no** form of the command.

**ip bootp server**

**no ip bootp server**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Enabled

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	11.2	This command was introduced.
	12.0(1)T	The DHCP relay agent and DHCP server features were introduced. BOOTP forwarding is now handled by the DHCP relay agent implementation.
	12.2(8)T	The <b>ip dhcp bootp ignore</b> command was introduced.

---



---

**Usage Guidelines** By default, the BOOTP service is enabled. When disabled, the **no ip bootp server** command will appear in the configuration file.

The integrated Dynamic Host Configuration Protocol (DHCP) server was introduced in Cisco IOS Release 12.0(1)T. Because DHCP is based on BOOTP, both of these services share the “well-known” UDP server port of 67 (per RFC 951, RFC 1534, and RFC 2131; the client port is 68). To disable DHCP services (DHCP relay and DHCP server), use the **no service dhcp** command. To disable BOOTP services (in releases 12.2(8)T and later), but leave DHCP services enabled, use the **ip dhcp bootp ignore** command.

If both the BOOTP server and DHCP server are disabled, “ICMP port unreachable” messages will be sent in response to incoming requests on port 67, and the original incoming packet will be discarded. If DHCP is enabled, using the **no ip bootp server** command by itself will not stop the router from listening on UDP port 67.



**Note**

---

As with all minor services, the async line BOOTP service should be disabled on your system if you do not have a need for it in your network.

Any network device that has User Data Protocol (UDP), TCP, BOOTP, DHCP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks.

---

---

**Examples**

In the following example, BOOTP and DHCP services are disabled on the router:

```
Router(config)# no ip bootp server
Router(config)# no service dhcp
```

---

**Related Commands**

Command	Description
<b>ip dhcp bootp ignore</b>	Configures the Cisco IOS DHCP server to selectively ignore and not reply to received Bootstrap Protocol (BOOTP) request packets, allowing you continue using DHCP while disabling BOOTP.
<b>service dhcp</b>	Enables the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server and relay agent features.

# ip director cache refresh

To enable the DistributedDirector Cache Auto Refresh function, use the **ip director cache refresh** command in global configuration mode. To disable automatic background refresh, use the **no** form of this command.

**ip director cache refresh**

**no ip director cache refresh**

**Syntax Description** This command has no keywords or arguments.

**Defaults** Automatic background refresh is disabled.

**Command Modes** Global configuration

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

**Usage Guidelines** The sorting cache on DistributedDirector must be enabled before you can use the **ip director cache refresh** command. To enable the sorting cache, use the **ip director cache** command.

Once automatic background refresh for the DistributedDirector cache is enabled, the cache will actively and continuously update every expired entry by processing a fake Domain Name System (DNS) request. The cache accumulates and updates answers to all past DNS queries received since cache auto refresh was initiated. Any repeat DNS request is always serviced directly from the cache.

**Examples** The following example enables automatic background refresh for the DistributedDirector cache:

```
Router(config)# ip director cache
Router(config)# ip director cache refresh

Router# show running-config

ip host myhost 172.2.2.10 172.2.2.20 172.2.2.30
.
.
.
ip director cache refresh
```

# ip director cache size

To configure the variable size of the DistributedDirector cache, use the **ip director cache size** command in global configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

**ip director cache size** *entries*

**no ip director cache size** *entries*

<b>Syntax Description</b>	<i>entries</i>	Maximum number of cache entries. Range is from 1 to 4294967295.
---------------------------	----------------	---

<b>Defaults</b>	Maximum number of cache entries: 2000
-----------------	---------------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(8)T	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>ip director cache size</b> command to configure the maximum number of cache entries that the DistributedDirector system will retain in its cache. This cache size is the maximum number of cache entries that are displayed when the user enters the <b>show ip director cache</b> command.
-------------------------	--

<b>Examples</b>	The following example configures the maximum number of cache entries:
-----------------	---

```
Router(config)# ip director cache size 1500
Cache size shrunk to 1500
```

```
Router# show ip director cache
Director cache is on
Cache current size = 0 maximum size = 1500
Cache time for sort cache entries: 60 secs
Director sort cache hits = 0
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip director cache</b>	Enables the sorting cache on DistributedDirector.
	<b>ip director cache time</b>	Configures how long the DistributedDirector system will retain per-client sorting information.

# ip director cache time

To configure how long the DistributedDirector system will retain per-client sorting information, use the **ip director cache time** command in global configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

**ip director cache time** *seconds*

**no ip director cache time** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Amount of time the per-client sorting information is retained, in number of seconds. Range is from 1 to 2147483. The default is 60 seconds.
---------------------------	----------------	---

<b>Defaults</b>	60 seconds
-----------------	------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(8)T	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>ip director cache time</b> command to specify how long the DistributedDirector system will retain per-client sorting in its cache. This cache time is the maximum amount of cache time displayed when the user enters the <b>show ip director cache</b> command.
-------------------------	---

<b>Examples</b>	The following example configures how long the DistributedDirector system will retain per-client sorting information:
-----------------	--

```
Router(config)# ip director cache time 100

Router# show ip director cache
Director cache is on
Cache current size = 0 maximum size = 2000
Cache time for sort cache entries: 100 secs
Director sort cache hits = 0
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip director cache</b>	Enables the sorting cache on DistributedDirector.
	<b>ip director cache size</b>	Configures the variable size of the DistributedDirector cache.

## ip director default priorities

To set a default priority for a specific metric on the DistributedDirector, use the **ip director default priorities** command in global configuration mode. To remove a default priority for a metric, use the **no** form of this command.

```
ip director default priorities [drp-int number] [drp-ext number] [drp-ser number]
[random number] [admin number] [drp-rtt number] [portion number] [availability number]
[route-map number] [boomerang number]
```

```
no ip director default priorities [drp-int number] [drp-ext number] [drp-ser number]
[random number] [admin number] [drp-rtt number] [portion number] [availability number]
[route-map number] [boomerang number]
```

Syntax Description	
<b>drp-int</b>	(Optional) DRP internal metric.
<i>number</i>	Numeric value of a priority level for a given metric. Range is from 1 to 100.
<b>drp-ext</b>	(Optional) DRP external metric.
<b>drp-ser</b>	(Optional) DRP server metric.
<b>random</b>	(Optional) Random metric.
<b>admin</b>	(Optional) Administrative metric.
<b>drp-rtt</b>	(Optional) DRP round-trip time metric.
<b>portion</b>	(Optional) Portion metric.
<b>availability</b>	(Optional) Availability metric.
<b>route-map</b>	(Optional) Route-map metric.
<b>boomerang</b>	(Optional) Boomerang metric.

**Defaults** No default priorities are specified.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(4)T	This command was introduced.
	12.2(8)T	The boomerang metric was added.

**Usage Guidelines** Not all of the metrics need to be specified, but at least one must be specified. If the boomerang metric is specified for a given host name, then all metrics of lower priority (that is, having a higher priority number) than boomerang are always ignored.

The default priorities specified will take effect if no priorities are specified in the **ip director host priority** command or in the corresponding Domain Name System (DNS) text record for the host.

To set the default priority for several metrics, enter the metric keywords and values to be configured on the same line as the **ip director default priorities** command.

**Examples**

In the following example, the boomerang metric is selected as the default priority:

```
Router(config)# ip director default priorities boomerang 1

Router# show running-config

ip host boom1 172.2.2.10 172.2.2.20 172.2.2.30
ip director server 172.2.2.20 drp-association 172.4.4.2
ip director server 172.2.2.30 drp-association 172.4.4.3
ip director server 172.2.2.10 drp-association 172.4.4.1
ip director host boom1
no ip director cache
ip dns primary boom1 soa boom1 boom1@com
ip director host boom1 priority boomerang 1
no ip director drp synchronized
```

**Related Commands**

Command	Description
<b>ip director access-list</b>	Defines an access list for DistributedDirector that specifies which subdomain names and host names should be sorted.
<b>ip director cache</b>	Enables the sorting cache on DistributedDirector.
<b>ip director default priorities</b>	Sets a default priority for a specific metric on DistributedDirector.
<b>ip director default weights</b>	Configures default weight metrics for DistributedDirector.
<b>ip director host priority</b>	Configures the order in which DistributedDirector considers metrics when picking a server.
<b>ip director host weights</b>	Sets host-specific weights for the metrics that DistributedDirector uses to determine the best server within a specific host name.
<b>ip director server admin-pref</b>	Configures a per-service administrative preference value.
<b>ip director server portion</b>	Sets the portion value for a specific server.
<b>ip director server preference</b>	Specifies DistributedDirector preference of one server over others or takes a server out of service.
<b>show ip director default priority</b>	Verifies the default configurations of DistributedDirector metrics.
<b>show ip director default weights</b>	Shows DistributedDirector default weights.
<b>show ip director servers</b>	Displays DistributedDirector server preference information.

## ip director default weights

To configure default weight metrics for DistributedDirector, use the **ip director default weights** command in global configuration mode. To set the defaults to zero, use the **no** form of this command.

```
ip director default weights {[drp-int number] [drp-ext number] [drp-ser number]
[drp-rtt number] [random number] [admin number] [portion number] [availability number]
[route-map number]}
```

```
no ip director default weights {[drp-int number] [drp-ext number] [drp-ser number]
[drp-rtt number] [random number] [admin number] [portion number] [availability number]
[route-map number]}
```

Syntax Description	
<b>drp-int</b> <i>number</i>	<p>(Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric (<b>drp-ext</b>) to help determine the distance between the router and the client originating the DNS query.</p> <p>If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent.</p>
<b>drp-ext</b> <i>number</i>	<p>(Optional) DRP external metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful.</p>
<b>drp-ser</b> <i>number</i>	<p>(Optional) DRP server metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric (<b>drp-int</b>) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query.</p> <p>If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes.</p>
<b>drp-rtt</b> <i>number</i>	<p>(Optional) DRP round-trip time metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query.</p>

<b>random number</b>	(Optional) Random metric. The range is 1 to 100. This option selects a random number for each distributed server and defines the “best” server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents.
<b>admin number</b>	(Optional) Administrative metric. The range is 1 to 100. This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service.
<b>portion number</b>	(Optional) Portion metric. The range is 1 to 100. This option assigns a load “portion” to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time.
<b>availability number</b>	(Optional) Availability metric. The range is 1 to 65535. This option specifies the load information for the DistributedDirector. The default value is 65,535.
<b>route-map number</b>	(Optional) Route-map metric. The range is 1 to 100. This option specifies if a server should be offered to a client.

**Defaults**

No default weights are specified.  
The availability default value is 65535.

**Command Modes**

Global configuration

**Command History**

Release	Modification
11.1(18)IA	This command was introduced.
12.1(5)T	The availability and route-map metrics were added.
12.2(4)T3	The command name was changed slightly: <b>default weights</b> replaced <b>default-weights</b> .

**Usage Guidelines**

Not all the metrics need to be configured; however, at least one metric must be configured when this command is used.

Default weights are used for all host names sorted by the DistributedDirector. To override default weights for a certain host, specify host-specific weights in the private DNS server configuration.

When the associated metric is referenced in the sorting decision, it will always be multiplied by the appropriate metric weight. In this way, you can specify that some metrics be weighted more than others. You may determine the weights that you want to use through experimentation. The weights given do not need to add up to 100.

The new availability metric allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

**Examples**

The following command configures default weights for the internal and external metrics:

```
Router(config)# ip director default weight drp-int 10 drp-ext 90
```

**Related Commands**

Command	Description
<b>debug ip director parse</b>	Shows debugging information for DistributedDirector parsing of TXT information.
<b>debug ip director sort</b>	Shows debugging information for DistributedDirector IP address sorting.
<b>ip director access-list</b>	Defines an access list for the DistributedDirector that specifies which subdomain names and host names should be sorted.
<b>ip director cache</b>	Enables the sorting cache on the DistributedDirector.
<b>ip director default priorities</b>	Sets default priorities for a specific metric on the DistributedDirector.
<b>ip director drp rttprobe</b>	Sets the protocol used by DRP agents for RTT probing in DistributedDirector.
<b>ip director host priority</b>	Configures the order in which the DistributedDirector considers metrics when selecting a server.
<b>ip director host weights</b>	Sets host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name.
<b>ip director server admin-pref</b>	Configures a per-service administrative preference value.
<b>ip director server portion</b>	Sets the portion value for a specific server.
<b>ip director server preference</b>	Specifies DistributedDirector preference of one server over others or takes a server out of service.
<b>show ip director default priority</b>	Verifies the default configurations of DistributedDirector metrics.
<b>show ip director default weights</b>	Shows the DistributedDirector default weights.
<b>show ip director servers</b>	Displays the DistributedDirector server preference information.

## ip director dfp

To configure the DistributedDirector Dynamic Feedback Protocol (DFP) agent with which the DistributedDirector should communicate, use the **ip director dfp** command in global configuration mode. To turn off the DFP agent, use the **no** form of this command.

**ip director dfp** *ip-address* [*port*] [*retry number*] [**attempts** *seconds*] [**timeout** *seconds*]

**no ip director dfp** *ip-address* [*port*] [*retry number*] [**attempts** *seconds*] [**timeout** *seconds*]

### Syntax Description

<i>ip-address</i>	IP address.
<i>port</i>	(Optional) Port number to which the distributed servers are configured. The default value is 8080.
<b>retry number</b>	(Optional) Number of times a connection will be attempted. The default value is 5 attempts.
<b>attempts</b> <i>seconds</i>	(Optional) Delay, in seconds, between each attempt. The default value is 10,000 seconds.
<b>timeout</b> <i>seconds</i>	(Optional) Maximum amount of time, in seconds, for which DFP information is assumed valid. The default value is 10,000 seconds.

### Defaults

The port default value is 8080.  
 The retry default value is 5 attempts.  
 The attempts default value is 10000 seconds.  
 The timeout default value is 10000 seconds.

### Command Modes

Global configuration

### Command History

Release	Modification
12.1(5)T	This command was introduced.

### Usage Guidelines

A connection is attempted a specified number of times with a delay of a specified number of seconds between each attempt. Once a connection is established, the DFP protocol will run. If a time interval update has not occurred for this DFP session, the connection breaks and is reestablished as described above.

### Examples

The following example configures the DistributedDirector to communicate with a specified DFP agent:

```
ip director dfp 10.0.0.1 retry 3 attempts 60 timeout 6000
```

## ip director dfp security

To configure a security key for use when connecting to the Dynamic Feedback Protocol (DFP) client named, use the **ip director dfp security** command in global configuration mode. To turn off the security key, use the **no** form of this command.

```
ip director dfp security ip-address md5 string [timeout]
```

```
no ip director dfp security ip-address md5 string [timeout]
```

Syntax Description		
	<i>ip-address</i>	IP address for the service.
	<b>md5</b>	Security data authentication. Message Digest 5.
	<i>string</i>	Security key.
	<i>timeout</i>	(Optional) Amount of time, in seconds, during which DistributedDirector will continue to accept a previously defined security key. The default value is 0 seconds.

**Defaults** The timeout default value is 0 seconds.

**Command Modes** Global configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced.

**Usage Guidelines** The **ip director dfp security** command should be entered before configuring the **ip director dfp** command, resulting in a connection being made, but it can be entered independently of making a connection.

DFP allows servers to take themselves Out-of-Service and place themselves back In-Service. This function could result in a security risk because a network that is hacked could be shut down even though all the servers are still performing. An optional security vector is included in DFP to allow each message to be verified. The security vector is used to describe the security algorithm being used and to provide the data for that algorithm. The security vector itself is also extensible in that it specifies which security algorithm is being used. This specification allows different levels of security from MD5 to Data Encryption Standard (DES) to be used without overhauling the protocol and disrupting any installed base of equipment. If a receiving unit is configured for the specified security type, all DFP packets must contain that security vector or they are ignored. If a receiving unit is not configured for any security type, the security vector does not have to be present, and if it is present, it is ignored while the rest of the message is processed normally.

**Examples** The following example configures the security key hello:

```
ip director dfp security 10.0.0.1 md5 hello 60
```

Related Commands

Command	Purpose
<b>ip director dfp</b>	Configures the DistributedDirector DFP agent with which the DistributedDirector should communicate.

# ip director drp rttprobe

To set the protocol used by Director Response Protocol (DRP) agents for round-trip time (RTT) probing in DistributedDirector, use the **ip director drp rttprobe** command in global configuration mode. To disable the use of a protocol, use the **no** form of the command.

```
ip director drp rttprobe [tcp | icmp]
```

```
no ip director drp rttprobe [tcp | icmp]
```

Syntax Description	tcp	(Optional) Transmission Control Protocol. This is the default.
	<b>icmp</b>	(Optional) Internet Control Message Protocol.

Defaults	TCP
----------	-----

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

Command History	Release	Modification
	12.2(4)T	This command was introduced.

**Usage Guidelines** Both protocols can be activated, in which case DistributedDirector will instruct DRP agents to return the RTT collected from either the TCP or Internet Control Message Protocol (ICMP) protocol, whichever becomes available first. At any time, at least one of the protocols must be active.

To use only one protocol, enable the protocol you want to use, and then disable the protocol that was already configured.

```
Router(config)# ip director drp rttprobe icmp
Router(config)# no ip director drp rttprobe tcp
```

**Examples** The following example shows that ICMP is configured for use by DRP agents for RTT probing:

```
Router(config)# ip director drp rttprobe icmp
```

Related Commands	Command	Description
	<b>ip director access-list</b>	Defines an access list for the DistributedDirector that specifies which subdomain names and host names should be sorted.
	<b>ip director cache</b>	Enables the sorting cache on the DistributedDirector.
	<b>ip director default priorities</b>	Sets default priorities for a specific metric on the DistributedDirector.
	<b>ip director default weights</b>	Configures default weight metrics for the DistributedDirector.

Command	Description
<b>ip director host priority</b>	Configures the order in which the DistributedDirector considers metrics when selecting a server.
<b>ip director host weights</b>	Sets host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name.
<b>ip director server admin-pref</b>	Configures a per-service administrative preference value.
<b>ip director server portion</b>	Sets the portion value for a specific server.
<b>ip director server preference</b>	Specifies DistributedDirector preference of one server over others or takes a server out of service.
<b>show ip director default priority</b>	Verifies the default configurations of DistributedDirector metrics.
<b>show ip director default weights</b>	Shows the DistributedDirector default weights.
<b>show ip director servers</b>	Displays the DistributedDirector server preference information.

# ip director drp synchronized

To activate clock synchronization between DistributedDirector and Director Response Protocol (DRP), use the **ip director drp synchronized** command in global configuration mode. To deactivate synchronization between the clocks in DistributedDirector and the DRPs, use the **no** form of this command.

**ip director drp synchronized**

**no ip director drp synchronized**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Clock synchronization is deactivated.

**Command Modes** Global configuration

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

**Usage Guidelines** This command is used in conjunction with boomerang racing.

When the **ip dir drp synchronized** command is configured, DistributedDirector specifies an absolute time at which the DRP agent should respond to the DNS client.

When **no ip director drp synchronized** is configured (which is the default), DistributedDirector specifies a relative time (based on the delay measured between DistributedDirector and the DRP agent) at which the DRP agent should respond to the Domain Name Service (DNS) client.

**Examples** In the following example, DistributedDirector and DRP clock synchronization are activated:

```
Router(config)# ip director drp synchronized

Router(config)# show running-config

ip host boom1 172.2.2.10 172.2.2.20 172.2.2.30
ip director server 172.2.2.20 drp-association 172.4.4.2
ip director server 172.2.2.30 drp-association 172.4.4.3
ip director server 172.2.2.10 drp-association 172.4.4.1
ip director host boom1
.
.
ip director drp synchronized
```

## ip director host priority

To configure the order in which the DistributedDirector considers metrics when picking a server, use the **ip director host priority** command in global configuration mode. To turn off metric priorities, use the **no** form of this command.

```
ip director host host-name priority {[drp-int number] [drp-ext number] [drp-ser number]
[drp-rtt number] [random number] [admin number] [portion number] [availability number]
[route-map number]}
```

```
no ip director host host-name priority {[drp-int number] [drp-ext number] [drp-ser number]
[drp-rtt number] [random number] [admin number] [portion number] [availability number]
[route-map number]}
```

### Syntax Description

<i>host-name</i>	Name of the host that maps to one or more IP addresses. Use the <i>host-name</i> argument to name the host that maps to one or more IP addresses. Do not use an IP address.
<b>drp-int</b> <i>number</i>	(Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100.  This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric ( <b>drp-ext</b> ) to help determine the distance between the router and the client originating the DNS query.  If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent.
<b>drp-ext</b> <i>number</i>	(Optional) DRP external metric. The range is 1 to 100.  This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful.
<b>drp-ser</b> <i>number</i>	(Optional) DRP server metric. The range is 1 to 100.  This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric ( <b>drp-int</b> ) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query.  If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes.

<b>drp-rtt</b> <i>number</i>	(Optional) DRP round-trip time metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query.
<b>random</b> <i>number</i>	(Optional) Random metric. The range is 1 to 100. This option selects a random number for each distributed server and defines the “best” server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents.
<b>admin</b> <i>number</i>	(Optional) Administrative metric. The range is 1 to 100. This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service.
<b>portion</b> <i>number</i>	(Optional) Portion metric. The range is 1 to 100. This option assigns a load “portion” to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time.
<b>availability</b> <i>number</i>	(Optional) Availability metric. The range is 1 to 65,535. This option specifies the load information for the DistributedDirector. The default value is 65,535.
<b>route-map</b> <i>number</i>	(Optional) Route-map metric. The range is 1 to 100. This option specifies if a server should be offered to a client.

**Defaults**

The availability default value is 65,535.

**Command Modes**

Global configuration

**Command History**

Release	Modification
11.1(18)IA	This command was introduced.
12.1(5)T	This command was integrated into 12.1 T. The <b>availability</b> and <b>route-map</b> metrics were added.
12.2(8)T	The <b>boomerang</b> metric was added.

**Usage Guidelines**

Not all of the metrics need to be specified, but at least one must be specified. If the boomerang metric is specified at a given priority level, then all other metrics of lower priority (that is, having a higher priority number) for that host name are ignored. If the boomerang metric is being considered, then it is the final step in determining the best server.

The **availability** keyword allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

If multiple servers end up with the same metric value, the next metric is considered to determine the “best” server. If multiple metrics have the same priority value, the metrics are added to obtain a *composite metric*. For example, if two metrics have the same priority value, they are first multiplied by their weight values (if specified) and then added together to form the composite metric.

If you do not specify weights for a group of distributed servers, there are no default weights for the Director, and if you have specified priority values, the weight values are set to 1.

Any metrics that have a nonzero weight and that are assigned no priority value are set to a priority value of 101. They are considered after all other metrics that have priority values. As a result, if no priority values are specified for any metric, metrics are treated additively to form one composite metric.

If you do not use priority and multiple servers have the same metric value, the server whose last IP address was looked at will be returned as the “best” server. If you want to return a random IP address in the case of a tie, use metric priority with the **random** metric as the last criterion.

To turn off all priorities on all metrics associated with the defined host name, use the **no ip director host priority** command. You can turn off the priority for a specific metric or metrics using the **no ip director host host-name priority [drp-int number] [drp-ext number] [drp-ser number] [drp-rtt number] [random number] [admin number] [portion number] [availability number] [route-map number]** command.

## Examples

The following example sets the external metric as the first priority and the administrative metric as the second priority:

```
Router(config)# ip director host www.xyz.com priority drp-ext 1 admin 2
```

The following example specifies the per-host priority of the metric, with a host named boom1, where the DRP internal metric is specified with a priority number of 1 and boomerang is specified with a priority number of 2:

```
Router(config)# ip director host BOOM1 priority drp-int 1 boomerang 2
```

```
Router(config)# do show running-config
```

```
ip host BOOM1 172.2.2.10 172.2.2.20 172.2.2.30
.
.
.
ip director host BOOM1
no ip director cache
ip dns primary boom1 soa boom1 boom1@com
ip director host boom1 priority drp-int 1 boomerang 2
```

## Related Commands

Command	Description
<b>ip director default priorities</b>	Sets a default priority for a specific metric on DistributedDirector.
<b>ip director default weights</b>	Configures default weight metrics for DistributedDirector.
<b>ip director host connect</b>	Enables the DistributedDirector to verify that a server is available.
<b>ip director host weights</b>	Sets host-specific weights for the metrics that DistributedDirector uses to determine the best server within a specific host name.
<b>show ip director default priority</b>	Verifies the default configurations of DistributedDirector metrics.

Command	Description
<b>show ip director default weights</b>	Shows DistributedDirector default weights.
<b>show ip director hosts</b>	Displays DistributedDirector host information.

## ip director host weights

To set host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name, use the **ip director host weights** command in global configuration mode. To turn off weights for a host, use the **no** form of this command.

```
ip director host host-name weights {[drp-int number] [drp-ext number] [drp-ser number]
[drp-rtt number] [random number] [admin number] [portion number] [availability number]
[route-map number]}
```

```
no ip director host host-name weights {[drp-int number] [drp-ext number] [drp-ser number]
[drp-rtt number] [random number] [admin number] [portion number] [availability number]
[route-map number]}
```

### Syntax Description

<i>host-name</i>	Name of the host that maps to one or more IP addresses. Do not use an IP address.
<b>drp-int</b> <i>number</i>	(Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100.  This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric ( <b>drp-ext</b> ) to help determine the distance between the router and the client originating the DNS query.  If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent.
<b>drp-ext</b> <i>number</i>	(Optional) DRP external metric. The range is 1 to 100.  This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful.
<b>drp-ser</b> <i>number</i>	(Optional) DRP server metric. The range is 1 to 100.  This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric ( <b>drp-int</b> ) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query.  If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes.

<b>drp-rtt</b> <i>number</i>	(Optional) DRP round-trip time metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query.
<b>random</b> <i>number</i>	(Optional) Random metric. The range is 1 to 100. This option selects a random number for each distributed server and defines the “best” server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents.
<b>admin</b> <i>number</i>	(Optional) Administrative metric. The range is 1 to 100. This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service.
<b>portion</b> <i>number</i>	(Optional) Portion metric. The range is 1 to 100. This option assigns a load “portion” to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time.
<b>availability</b> <i>number</i>	(Optional) Availability metric. The range is 1 to 65,535. This option specifies the load information for the DistributedDirector. The default value is 65,535.
<b>route-map</b> <i>number</i>	(Optional) Route-map metric. The range is 1 to 100. This option specifies if a server should be offered to a client.

**Note**

No host weights are set. If the **ip director default-weights** command is configured, the configured weights are the default.

**Defaults**

The availability default value is 65,535.

**Command Modes**

Global configuration

**Command History**

Release	Modification
11.1(25)IA	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)T	The <b>availability</b> and <b>route-map</b> metrics were added.

**Usage Guidelines**

Use host-specific weights when you want to use different metric weights for different virtual host names (for example, www.xyz.com and ftp.xyz.com).

The new availability metric allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

If desired, host-specific weights can instead be configured on the DistributedDirector default DNS server.

For example, you could configure host-specific weights with the following DNS TXT record:

```
hostname in txt "ciscoDD: weights {[drp-int number] [drp-ext number] [drp-ser number]
[random number] [admin number]}"
```

To use the default weights for all metrics associated with this host name, use the **no ip director host weights** command. To use the default weights for a specific metric or metrics, use the **no ip director host host-name weights [drp-int number] [drp-ext number] [drp-ser number] [drp-rtt number] [random number] [admin number] [portion number] [availability number] [route-map number]** command.

---

### Examples

The following example sets the DRP internal metric to 4:

```
Router(config)# ip director host www.xyz.com weights drp-int 4
```

---

### Related Commands

Command	Description
<b>ip director default-weights</b>	Configures default weight metrics for the DistributedDirector.
<b>show ip director dfp</b>	Displays information about the current status of the DistributedDirector connections with a particular DFP agent.

# ip director server availability

To configure a default availability value for all ports on a server, use the **ip director server availability** command in global configuration mode. To restore the default, use the **no** form of this command.

```
ip director server ip-address availability {availability-value | dfp [availability-value]}
```

```
no ip director server ip-address availability {availability-value | dfp [availability-value]}
```

Syntax Description		
<i>ip-address</i>		IP address.
<i>availability-value</i>		Availability value as it would be represented on the DistributedDirector system. The range is 0 to 65,535.
<b>dfp</b> [ <i>availability-value</i> ]		Availability value as it would be represented on the LocalDirector system. The range for value is 0 to 65,535.

**Defaults** The availability default value is 65,535.

**Command Modes** Global configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced.

**Usage Guidelines** There are two methods for specifying a default availability value. These two methods exist because the LocalDirector and the DistributedDirector deal with values in two different ways. All metrics for the DistributedDirector are arranged such that lower is better; however the LocalDirector load information is calculated such that higher is better. Thus, the DistributedDirector translates the metric value upon receipt from the LocalDirector by subtracting the availability from the maximum possible value of 65,535.

**Examples** To configure a default availability to be used if there is no other valid availability information, the following configuration would suffice. The following example shows how to specify the LocalDirector load and DistributedDirector availability, respectively:

```
ip director server 10.0.0.1 availability dfp 1
ip director server 10.0.0.1 availability 65534
```

To make the availability clear and to allow for specifying numbers in both schemes easily, there are two methods of specifying availability information. If the servers are running multiple serves, it may be necessary to configure the default availability value on a per-port basis by using the **ip director server port availability** command.

```
ip director server 10.0.0.1 port availability dfp 65535
ip director server 10.0.0.20 port availability dfp 65535
```

---

Related Commands

Command	Description
<b>ip director server port availability</b>	Configures a default availability value for a specific port on a server.

# ip director server port availability

To configure a default availability value for a specific port on a server, use the **ip director server port availability** command in global configuration mode. To restore the default, use the **no** form of this command.

```
ip director server ip-address port availability { availability-value | dfp [availability-value] }
```

```
no ip director server ip-address port availability { availability-value | dfp [availability-value] }
```

Syntax Description		
	<i>ip-address</i>	IP address.
	<i>availability-value</i>	Availability value as it would be represented on the DistributedDirector system. The range is 0 to 65,535.
	<b>dfp</b> [ <i>availability-value</i> ]	Availability value as it would be represented on the LocalDirector system. The range for value is 0 to 65,535.

**Defaults** The availability default value is 65,535.

**Command Modes** Global configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced.

**Usage Guidelines** There are two methods for specifying a default availability value. These two methods exist because the LocalDirector and the DistributedDirector deal with values in two different ways. All metrics for the DistributedDirector are arranged such that lower is better; however the LocalDirector load information is calculated such that higher is better. Thus, the DistributedDirector translates the metric value upon receipt from the LocalDirector by subtracting the availability from the maximum possible value of 65,535.

**Examples** To make the availability clear and to allow for specifying numbers in both schemes easily, there are two methods of specifying availability information. If the servers are running multiple serves, it may be necessary to configure the default availability value on a per-port basis by using the **ip director server port availability** command.

```
ip director server 10.0.0.1 port availability dfp 65535
ip director server 10.0.0.20 port availability dfp 65535
```

To configure a default availability to be used if there is no other valid availability information, the following configuration would suffice. The following example shows how to specify the LocalDirector load and DistributedDirector availability, respectively:

```
ip director server 10.0.0.1 availability dfp 1
ip director server 10.0.0.1 availability 65534
```

Related Commands

Command	Description
<b>ip director server availability</b>	Configures a default availability value for all ports on a server.

# ip dns server

To enable the Domain Name System (DNS) server on a router, use the **ip dns server** command in global configuration mode. To disable the DNS server, use the **no** form of the command.

**ip dns server**

**no ip dns server**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The DNS server is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(4)T	This command was introduced.

**Usage Guidelines** Use the command to enable the DNS server as needed.

**Examples** In the following example, the DNS server is enabled:

```
Router(config)# ip dns server
```

# ip drp domain

To add a new domain to the DistributedDirector client or to configure an existing domain, use the **ip drp domain** command in global configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

**ip drp domain** *domain-name*

**no ip drp domain** *domain-name*

## Syntax Description

<i>domain-name</i>	Specified domain name.
--------------------	------------------------

## Defaults

No default domain is configured.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

Enabling this command puts the client in boomerang configuration mode.

Use the **ip drp domain** command to enter a new or existing domain name. Entering a new domain name creates a new domain, and entering an existing domain name allows the user to configure the specified domain. When a domain name is configured on the boomerang client, the user can configure specific parameters, such as server address, aliases, and time to live (TTL) values, for that domain.

When a Director Response Protocol (DRP) agent receives a Domain Name System (DNS) racing message from boomerang servers such as DistributedDirector, the DRP agent extracts the specified domain name (for example, www.cisco.com) in the DNS message.

## Examples

In the following example, a domain named “www.boom1.com” is added on the boomerang client:

```
Router(config)# ip drp domain www.boom1.com
```

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

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>alias (boomerang)</b>	Configures an alias name for a specified domain.
<b>server (boomerang)</b>	Configures the server address for a specified boomerang domain.
<b>show ip drp</b>	Displays DRP statistics on DistributedDirector or a DRP server agent.
<b>show ip drp boomerang</b>	Displays boomerang information on the DRP agent.
<b>tll dns</b>	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.
<b>tll ip</b>	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

# ip finger

To configure a system to accept Finger protocol requests (defined in RFC 742), use the **ip finger** command in global configuration mode. To disable this service, use the **no** form of this command.

**ip finger [rfc-compliant]**

**no ip finger**

<b>Syntax Description</b>	<b>rfc-compliant</b>	(Optional) Configures the system to wait for “Return” or “/W” input when processing Finger requests. This keyword should not be used for those systems.
---------------------------	----------------------	---

<b>Defaults</b>	Disabled
-----------------	----------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3	This command was introduced.
	12.1(5), 12.1(5)T	This command was changed from being enabled by default to being disabled by default.

<b>Usage Guidelines</b>	<p>The Finger service allows remote users to view the output equivalent to the <b>show users [wide]</b> command.</p> <p>When <b>ip finger</b> is configured, the router will respond to a <b>telnet a.b.c.d finger</b> command from a remote host by immediately displaying the output of the <b>show users</b> command and then closing the connection.</p> <p>When the <b>ip finger rfc-compliant</b> command is configured, the router will wait for input before displaying anything (as required by RFC 1288). The remote user can then enter the Return key to display the output of the <b>show users EXEC</b> command, or enter <b>/W</b> to display the output of the <b>show users wide EXEC</b> command. After this information is displayed, the connection is closed.</p>
-------------------------	--



**Note**

As with all minor services, the Finger service should be disabled on your system if you do not have a need for it in your network.

Any network device that has UDP, TCP, BOOTP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks.

Because of the potential for hung lines, the **rfc-compliant** form of this command should not be configured for devices with more than 20 simultaneous users.

<b>Examples</b>	The following example disables the Finger protocol:
-----------------	---

```
Router(config)# no ip finger
```

# ip ftp passive

To configure the router to use only passive FTP connections, use the **ip ftp passive** command in global configuration mode. To allow all types of FTP connections, use the **no** form of this command.

**ip ftp passive**

**no ip ftp passive**

**Syntax Description** This command has no arguments or keywords.

**Defaults** All types of FTP connections are allowed.

**Command Modes** Global configuration

Release	Modification
10.3	This command was introduced.

**Examples** In the following example, the router is configured to use only passive FTP connections:

```
Router(config)# ip ftp passive
```

Command	Description
<b>ip ftp password</b>	Specifies the password to be used for FTP connections.
<b>ip ftp source-interface</b>	Specifies the source IP address for FTP connections.
<b>ip ftp username</b>	Configures the username for FTP connections.

