

# sntp broadcast client

To use the Simple Network Time Protocol (SNTP) to accept Network Time Protocol (NTP) traffic from any broadcast server, use the **sntp broadcast client** command in global configuration mode to configure a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router. To prevent the router from accepting broadcast traffic, use the **no** form of this command.

**sntp broadcast client**

**no sntp broadcast client**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The router does not accept SNTP traffic from broadcast servers.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

SNTP is a compact, client-only version of the NTP. SNMP can only receive the time from NTP servers; it cannot be used to provide time services to other systems.

SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although you can configure extended access lists to provide some protection.

You must configure the router with either this command or the **sntp server** global configuration command to enable SNTP.

## Examples

The following example enables the router to accept broadcast NTP packets and shows sample **show sntp** command output:

```
Router(config)# sntp broadcast client
Router(config)# end
Router#
%SYS-5-CONFIG: Configured from console by console
Router# show sntp
SNTP server      Stratum    Version    Last Receive
172.21.28.34     4          3          00:00:36   Synced   Bcast
```

Broadcast client mode is enabled.

Related Commands	Command	Description
	<b>show sntp</b>	Displays information about SNTP on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.
	<b>sntp server</b>	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to request and accept NTP traffic from a time server.

# sntp logging

To enable Simple Network Time Protocol (SNTP) message logging, use the **sntp logging** command in global configuration mode. To disable SNTP logging, use the **no** form of this command.

**sntp logging**

**no sntp logging**

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

**Defaults** SNTP message logging is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.3(7)T	This command was introduced.

**Usage Guidelines** Use the **sntp logging** command to control the display of SNTP logging messages. SNTP is a compact, client-only version of Network Time Protocol (NTP). SNTP can be used only to receive the time from NTP servers; SNTP cannot be used to provide time services to other systems. You should consider carefully the use of SNTP rather than NTP in primary servers.

**Examples** The following example shows how to enable SNTP message logging, configure the IP address of the SNTP server as 10.107.166.3, and verify that SNTP logging is enabled:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# sntp logging

Router(config)# sntp server 10.107.166.3

Router(config)# end

Router#
04:02:54: %SYS-5-CONFIG_I: Configured from console by console
Router#

Router# show running-config | include ntp

sntp logging
sntp server 10.107.166.3
```

The “sntp logging” entry in the configuration file verifies that SNTP message logging is enabled.

The following example shows how to disable SNTP message logging and verify that it is disabled:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# no sntp logging

Router(config)# end

Router#

04:04:34: %SYS-5-CONFIG_I: Configured from console by console

Router# show running-config | include ntp

sntp server 10.107.166.3
```

The “sntp logging” entry no longer appears in the configuration file, which verifies that SNTP message logging is disabled.

#### Related Commands

Command	Description
<b>show sntp</b>	Displays information about SNTP on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.
<b>sntp broadcast client</b>	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to accept NTP traffic from any broadcast server.
<b>sntp server</b>	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to request and accept NTP traffic from a time server.

# sntp server

To configure a Cisco 800, Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use the Simple Network Time Protocol (SNTP) to request and accept Network Time Protocol (NTP) traffic from a stratum 1 time server, use the **sntp server** command in global configuration mode. To remove a server from the list of NTP servers, use the **no** form of this command.

```
sntp server {address | hostname} [version number]
```

```
no sntp server {address | hostname}
```

## Syntax Description

<i>address</i>	IP address of the time server.
<i>hostname</i>	Host name of the time server.
<b>version number</b>	(Optional) Version of NTP to use. The default is 1.

## Defaults

The router does not accept SNTP traffic from a time server.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

SNTP is a compact, client-only version of the NTP. SNMP can only receive the time from NTP servers; it cannot be used to provide time services to other systems.

SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although you can configure extended access lists to provide some protection.

Enter this command once for each NTP server.

You must configure the router with either this command or the **sntp broadcast client** global configuration command in order to enable SNTP.

SNTP time servers should operate only at the root (stratum 1) of the subnet, and then only in configurations where no other source of synchronization other than a reliable radio or modem time service is available. A stratum 2 server cannot be used as an SNTP time server. The use of SNTP rather than NTP in primary servers should be carefully considered.

**Examples**

The following example enables the router to request and accept NTP packets from the server at 172.21.118.9 and displays sample **show sntp** command output:

```
Router(config)# sntp server 172.21.118.9
Router(config)# end
Router#
%SYS-5-CONFIG: Configured from console by console
Router# show sntp

SNTP server      Stratum   Version   Last Receive
172.21.118.9    5         3         00:01:02   Synced
```

**Related Commands**

Command	Description
<b>show sntp</b>	Displays information about SNTP on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.
<b>sntp broadcast client</b>	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to accept NTP traffic from any broadcast server.

# sntp source-interface

To use a particular source address in Simple Network Time Protocol (SNTP) packets, use the **sntp source-interface** command in global configuration mode. To remove the specified source address, use the **no** form of this command.

**sntp source-interface** *type number*

**no sntp source-interface**

## Syntax Description

<i>type</i>	Type of interface.
<i>number</i>	Number of the interface.

## Command Default

The source address is determined by the outgoing interface.

## Command Modes

Global configuration

## Command History

Release	Modification
12.4(10)	This command was introduced.

## Usage Guidelines

Use this command to specify a particular source IP address for all SNTP packets. The address is taken from the named interface. This command is useful if the address on an interface cannot be used as the destination for reply packets. The **no** form of the command only replaces the default; that is, the source address of the SNTP request sent is determined by the outgoing interface.

If this command is the last one issued and you then remove it, the SNTP process stops.

## Examples

The following example shows how to configure a router to use the IP address of interface Ethernet 0 as the source address for all outgoing SNTP packets:

```
Router(config)# sntp source-interface ethernet 0
```

The following example shows how to remove a configured SNTP option:

```
Router(config)# no sntp source-interface
```

# spec-file install add-entry

To copy a spec file entry (SFE) from a remote location and add it to the local spec file, use the **spec-file install add-entry** command in privileged EXEC mode.

```
spec-file install [force] location:local-filename add-entry url:remote-filename command
```

Syntax Description		
<b>force</b>	(Optional)	Performs the action without prompting.
<i>location:local-filename</i>	Spec filename, which must be on a local file system. Valid locations are <b>bootflash:</b> , <b>flash:</b> , <b>nvram:</b> , and any valid disk or slot number (such as <b>disk0:</b> or <b>slot1:</b> ).	Spec files have a .odm suffix. You will be prompted to confirm adding the SFE, unless the optional <b>force</b> keyword is used.
<i>url:remote-filename</i>	Location (URL) and filename of the remote spec file. Valid URLs are <b>archive:</b> , <b>bootflash:</b> , <b>cns:</b> , <b>flash:</b> , <b>ftp:</b> , <b>http:</b> , <b>null:</b> , <b>nvram:</b> , <b>pram:</b> , <b>rcp:</b> , <b>scp:</b> , <b>system:</b> , <b>tar:</b> , <b>tftp:</b> , <b>tmpsys:</b> , and any valid disk or slot number (such as <b>disk0:</b> or <b>slot1:</b> ).	
<i>command</i>	Command	SFE to be added to the spec file.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	12.4(20)T	This command was introduced.
	12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

**Usage Guidelines** Use the **spec-file install add-entry** command to add an SFE to a spec file. A check is performed on the loaded SFE to ensure that the command is not already present in the spec file, and that the SFE can be parsed correctly in Extensible Markup Language (XML).

If the spec file does not exist, you will be prompted before the file is created. If the command SFE already exists in the spec file, you will be prompted before the command SFE is replaced. A backup copy of the local spec file is created before the remote SFE is added.

**Examples** The following example adds the **show arp** command SFE from the remote show\_arp.odm file at location “tftp://system1/user1” to the local file:

```
Router# spec-file install slot0:spec_file.odm add-entry tftp://system1/user1/show_arp.odm show arp
```

Unless you add the **force** keyword to the command string, you will be prompted as follows:

```
create new spec file? [yes]:  
CLI exists, delete it? [yes]:
```

Pressing the **Enter** key is the same as typing **yes**. Type **no** and press **Enter** to stop either process.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>spec-file install built-in</b>	Replaces the current spec file with the built-in spec file.
	<b>spec-file install file</b>	Replaces a local spec file with a remote spec file.
	<b>spec-file install remove-entry</b>	Removes an SFE from a spec file.
	<b>spec-file install restore</b>	Restores a spec file to its previous contents using a backup file.

# spec-file install built-in

To replace the current spec file with the built-in spec file, use the **spec-file install built-in** command in privileged EXEC mode.

**spec-file install** [**force**] *location:local-filename* **built-in**

## Syntax Description

<b>force</b>	(Optional) Performs the action without prompting.
<i>location:local-filename</i>	Spec filename, which must be on a local file system. Valid locations are <b>bootflash:</b> , <b>flash:</b> , <b>nvrn:</b> , and any valid disk or slot number (such as <b>disk0:</b> or <b>slot1:</b> ).  Spec files have a .odm suffix.  If <i>local-filename</i> exists, you will be prompted for a yes or no response before the file is replaced, unless the optional <b>force</b> keyword is used.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

## Usage Guidelines

Use the **spec-file install built-in** command to replace the current spec file with the built-in spec file. You will be prompted before the current file is replaced and *filename.bak* will be created.

## Examples

The following example shows how to start the process to replace the current spec file with the built-in spec file:

```
Router# spec-file install slot0:spec_file.odm built-in
```

Unless you add the **force** keyword to the command string, you will be prompted as follows:

```
Replace existing file? [yes]:
```

Press the **Enter** key to make a backup copy of the current file and then replace it with the built-in spec file. Type **no** and press **Enter** to stop the process.

## Related Commands

Command	Description
<b>spec-file install add-entry</b>	Copies an SFE from a remote location and adds it to a local spec file.
<b>spec-file install file</b>	Replaces a local spec file with a remote spec file.
<b>spec-file install remove-entry</b>	Removes an SFE from a spec file.
<b>spec-file install restore</b>	Restores a spec file to its previous contents using a backup file.

# spec-file install file

To replace a local spec file with a remote spec file, use the **spec-file install file** command in privileged EXEC mode.

**spec-file install** [**force**] *location:local-filename* **file** *url:remote-filename*

Syntax Description	
<b>force</b>	(Optional) Performs the action without prompting.
<i>location:local-filename</i>	Spec filename, which must be on a local file system. Valid locations are <b>bootflash:</b> , <b>flash:</b> , <b>nvrाम:</b> , and any valid disk or slot number (such as <b>disk0:</b> or <b>slot1:</b> ).  Spec files have a .odm suffix.  When <i>local-filename</i> exists, you will be prompted for a yes or no response before the file is copied, unless the optional <b>force</b> keyword is used.
<i>url:remote-filename</i>	Location (URL) and filename of the remote spec file. Valid URLs are <b>archive:</b> , <b>bootflash:</b> , <b>cns:</b> , <b>flash:</b> , <b>ftp:</b> , <b>http:</b> , <b>null:</b> , <b>nvrाम:</b> , <b>pram:</b> , <b>rep:</b> , <b>scp:</b> , <b>system:</b> , <b>tar:</b> , <b>tftp:</b> , <b>tmpsys:</b> , and any valid disk or slot number (such as <b>disk0:</b> or <b>slot1:</b> ).

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	12.4(20)T	This command was introduced.
	12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

**Usage Guidelines** Use the **spec-file install file** command to copy a remote spec file to a local spec file. A check of the loaded file is performed to ensure that each specified command is included only once, and that the spec file entry (SFE) can be parsed correctly in Extensible Markup Language (XML).

**Examples** The following example shows how to copy a remote spec file on “tftp://system1/user1” to the local file:

```
Router# spec-file install slot0:spec_file.odm file tftp://system1/user1/spec_file.odm
```

Unless you add the **force** keyword to the command string, you will be prompted as follows:

```
Replace existing file? [yes]:
```

Press the **Enter** key to complete the command. Type **no** and press **Enter** to stop the process.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>spec-file install add-entry</b>	Copies an SFE from a remote location and adds it to a local spec file.
<b>spec-file install built-in</b>	Replaces the current spec file with the built-in spec file.
<b>spec-file install remove-entry</b>	Removes an SFE from a spec file.
<b>spec-file install restore</b>	Restores a spec file to its previous contents using a backup file.

# spec-file install remove-entry

To remove a spec file entry (SFE) from a spec file, use the **spec-file install remove-entry** command in privileged EXEC mode.

**spec-file install** [**force**] *location:local-filename* **remove-entry** *command*

Syntax Description		
<b>force</b>	(Optional)	Performs the action without prompting.
<i>location:local-filename</i>	Spec filename, which must be on a local file system. Valid locations are <b>bootflash:</b> , <b>flash:</b> , <b>nvrn:</b> , and any valid disk or slot number (such as <b>disk0:</b> or <b>slot1:</b> ).	Spec files have a .odm suffix.
<i>command</i>	Command	SFE to be removed from the spec file.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	12.4(20)T	This command was introduced.
	12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

**Usage Guidelines** Use the **spec-file install remove-entry** command to remove a command SFE from a spec file. A check is performed to ensure that the command SFE is present in the spec file. If the spec file does not exist, this command fails. A backup copy of the spec file is created before the SFE is removed.

**Examples** The following example shows how to remove the **show arp** command SFE from the remote show\_arp.odm file to the local spec\_file.odm file:

```
Router# spec-file install slot0:spec_file.odm remove-entry show arp
```

Related Commands	Command	Description
	<b>spec-file install add-entry</b>	Copies an SFE from a remote location and adds it to a local spec file.
	<b>spec-file install built-in</b>	Replaces the current spec file with the built-in spec file.
	<b>spec-file install file</b>	Replaces a local spec file with a remote spec file.
	<b>spec-file install restore</b>	Restores a spec file to its previous contents using a backup file.

# spec-file install restore

To restore a spec file to its previous contents using a backup file, use the **spec-file install restore** command in privileged EXEC mode.

```
spec-file install [force] location:local-filename restore
```

## Syntax Description

<b>force</b>	(Optional) Performs the action without prompting.
<i>location:local-filename</i>	Spec filename, which must be on a local file system. Valid locations are <b>bootflash:</b> , <b>flash:</b> , <b>nvram:</b> , and any valid disk or slot number (such as <b>disk0:</b> or <b>slot1:</b> ).  Spec files have a .odm suffix.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

## Usage Guidelines

Use the **spec-file install restore** command to revert a spec file to its original contents using a backup (.bak) file. If the .bak file does not exist, this command fails.

## Examples

The following example shows how to restore the spec file using the backup file:

```
Router# spec-file install slot0:spec_file.odm restore
```

## Related Commands

Command	Description
<b>spec-file install add-entry</b>	Copies an SFE from a remote location and adds it to a local spec file.
<b>spec-file install built-in</b>	Replaces the current spec file with the built-in spec file.
<b>spec-file install file</b>	Replaces a local spec file with a remote spec file.
<b>spec-file install remove-entry</b>	Removes an SFE from a spec file.

# startup (test boolean)

To specify whether an event can be triggered for the Boolean trigger test, use the **startup** command in event trigger boolean configuration mode. To disable the configured settings, use the **no** form of this command.

**startup**

**no startup**

---

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

---

**Command Default** The startup event is enabled when the Boolean trigger test is enabled.

---

**Command Modes** Event trigger boolean configuration (config-event-trigger-boolean)

---

**Command History**

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

---

**Usage Guidelines**

The **startup** command triggers an event when the conditions specified for the Boolean trigger test are met.

---

**Examples**

The following example shows how to specify startup for the Boolean trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name EventA
Router(config-event-trigger)# test boolean
Router(config-event-trigger-boolean)# startup
Router(config-event-trigger-boolean)#
```

---

**Related Commands**

Command	Description
<b>test</b>	Enables a trigger test.

## startup (test existence)

To specify whether an event can be triggered for the existence trigger test, use the **startup** command in event trigger existence configuration mode. To disable the configured settings, use the **no** form of this command.

```
startup {present | absent}
```

```
no startup {present | absent}
```

Syntax Description	present	absent
	Triggers the present startup test when the existence trigger conditions are met.	Triggers the absent startup test when the existence trigger conditions are met.

**Command Default** By default, both present and absent startup tests are triggered.

**Command Modes** Event trigger existence configuration (config-event-trigger-existence)

Command History	Release	Modification
	12.4(20)T	This command was introduced.
	12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

**Usage Guidelines** The **startup** command triggers an event when the conditions specified for the existence trigger test are met.

**Examples** The following example shows how to specify startup for the existence trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name EventA
Router(config-event-trigger)# test existence
Router(config-event-trigger-existence)# startup
Router(config-event-trigger-existence)#
```

Related Commands	Command	Description
	test	Enables a trigger test.

# startup (test threshold)

To specify whether an event can be triggered for the threshold trigger test, use the **startup** command in the threshold test configuration mode. To disable the configured settings, use the **no** form of this command.

**startup** { **rising** | **falling** | **rise-or-falling** }

**no startup**

## Syntax Description

<b>rising</b>	Specifies the rising threshold value to check against the set value during startup when the trigger type is threshold.
<b>falling</b>	Specifies the falling threshold value to check against the set value during startup when the trigger type is threshold.
<b>rise-or-falling</b>	Specifies the rising or falling threshold value to check against the set value during startup when the trigger type is threshold. This is the default value.

## Command Default

The rising or falling threshold value is checked against the set value during startup when the trigger type is threshold.

## Command Modes

Event trigger threshold configuration mode (config-event-trigger-threshold)

## Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

## Usage Guidelines

The **startup** command starts an event when the conditions for threshold trigger test are met.

## Examples

The following example shows how to specify startup for the threshold trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name EventA
Router(config-event-trigger)# test threshold
Router(config-event-trigger-threshold)# startup rising
Router(config-event-trigger-threshold)#
```

## Related Commands

Command	Description
<b>test</b>	Enables a trigger test.

# stealth

To disable the Web Services Management Agent (WSMA) from sending SOAP faults, use the **stealth** command in WSMA listener configuration mode. To enable WSMA to send the SOAP faults, use the **no** form of this command.

**stealth**

**no stealth**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Stealth is disabled; that is, SOAP faults are sent.

## Command Modes

WSMA listener configuration (config-wsma-listen)

## Command History

Release	Modification
12.4(24)T	This command was introduced.

## Usage Guidelines

Use this command from the WSMA listener configuration mode. To enter this mode, enter the **wsma profile listener** command in global configuration mode.

## Examples

The following example shows how to enable the **stealth** command to stop sending the SOAP faults:

```
Router(config)# wsma profile listener prof1
Router(config-wsma-listen)# stealth
Router(config-wsma-listen)#
```

## Related Commands

Command	Description
<b>acl</b>	Enables access control lists for restricting addresses that can connect to a WSMA profile.
<b>idle-timeout</b>	Sets a time for the WSMA profile to disconnect the session when there is no network traffic.
<b>max-message</b>	Sets the maximum size limit for incoming messages.
<b>transport</b>	Defines a transport configuration for a WSMA profile.
<b>wsma profile listener</b>	Configures and enables a WSMA listener profile.
<b>wsse</b>	Enables the WSSE for a WSMA profile.

# system (ERM policy)

To configure system level resource owners (ROs), use the **system** command in Embedded Resource Manager (ERM) policy configuration mode.

**system**

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

**Command Default** No system level ROs are configured.

**Command Modes** ERM policy configuration

Command History	Release	Modification
	12.3(14)T	This command was introduced.
	12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

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

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

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

# tclquit

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

## tclquit

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

**Defaults** The Tcl shell is disabled.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	12.3(2)T	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

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

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

Related Commands	Command	Description
	<b>tclsh</b>	Enables the interactive Tcl shell.
	<b>tclsafe</b>	Enables the interactive Tcl shell untrusted safe mode.

# tclsafe

To enable the interactive Tool Command Language (Tcl) shell untrusted safe mode, use the **tclsafe** command in privileged EXEC mode. To exit from the safe mode, use the **exit** or the **tclquit** command.

**tclsafe**

**exit | tclquit**

---

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

---

**Command Default** The Tcl shell untrusted safe mode is disabled.

---

**Command Modes** Privileged EXEC (#)

---

Command History	Release	Modification
	12.4(15)T	This command was introduced.

---



---

**Usage Guidelines** Use the **tclsafe** command when you want to manually run Tcl commands from the Cisco IOS command-line interface (CLI) in untrusted safe mode. When you use the **tclsafe** command and enter the interactive Tcl shell safe mode, you can explore the safe mode Tcl commands that are available. When a script fails the signature check for a configured trustpoint name, it is determined to be untrusted. Untrusted Tcl scripts execute in limited safe mode, if **scripting tcl trustpoint untrusted safe-execute** command is configured. In order to get a better understanding of what is available in this limited safe mode, use the **tclsafe** Exec command to explore the options.

After Tcl commands are entered they are sent to a Tcl interpreter. If the commands are recognized as valid Tcl commands, the command is executed and the result is sent to the tty. If a command is not a recognized Tcl command, it is sent to the Cisco IOS CLI parser. If the command is not a Tcl or Cisco IOS command, two error messages are displayed.

A predefined Tcl script can be created outside of Cisco IOS software, transferred to flash or disk memory, and run within Cisco IOS software. It is also possible to create a Tcl script and precompile the code before running it under Cisco IOS software. To exit from this mode, use the **exit** or the **tclquit** command to disable the use of the Tcl shell and return to privileged EXEC mode.

You can also use the **tclsafe** command with a script name such as **tclsafe disk0:hello.tcl**. The script **hello.tcl** executes immediately and allows you to exit from the untrusted safe mode and return to privileged EXEC mode.

---

**Examples** The following example shows how to enable the Tcl shell untrusted safe mode and run **info commands**:

```
Router# tclsafe
Router(safe)(tcl)# info commands
info commands
```

tell socket subst open eof glob list pid time eval lrange tcl\_trace fblocked lsearch gets  
 case lappend proc break variable llength return linsert error catch clock info split array  
 if fconfigure concat join lreplace source fcopy global switch update close cd for file  
 append format read package set binary namespace scan seek while flush after vwait uplevel  
 continue hostname foreach rename fileevent regexp upvar unset encoding expr load regsub  
 interp history puts incr lindex lsort string

The following example shows how to execute the script **hello.tcl** to exit from the untrusted safe mode and return to privileged EXEC mode.

```
Router# tclsafe disk0:hello.tcl
```

#### Related Commands

Command	Description
<b>scripting tcl trustpoint untrusted</b>	Allows the interactive Tcl scripts to run regardless of the scripts failing the signature check.
<b>tclquit</b>	Quits Tcl shell.
<b>tclsh</b>	Enables the interactive Tcl shell and enters Tcl configuration mode.

# tclsh

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

**tclsh**

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

**Defaults** The Tcl shell is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(2)T	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

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

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

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

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

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

## template (cns)

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

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

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

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

**Command Default** No CNS connect templates are specified.

**Command Modes** CNS connect configuration

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

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

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

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

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

**Examples**

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

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

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

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

**Related Commands**

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

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

# test (event trigger)

To specify the type of test to perform during an event trigger, use the **test** command in event trigger configuration mode. To disable the trigger test configuration settings, use the **no** form of this command.

**test** { **existence** | **boolean** | **threshold** }

**no test** { **existence** | **boolean** | **threshold** }

Syntax Description	Parameter	Description
	<b>existence</b>	Enables the existence trigger test.
	<b>boolean</b>	Enables the Boolean trigger test. Boolean test is the default trigger test performed during event triggers.
	<b>threshold</b>	Enables the threshold trigger test.

**Command Default** The Boolean trigger test is enabled by default.

**Command Modes** Event trigger configuration (config-event-trigger)

Command History	Release	Modification
	12.4(20)T	This command was introduced.
	12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

**Usage Guidelines** The trigger table in the Event MIB has supplementary tables for additional objects that are configured based on the type of test performed for the trigger. For each trigger entry type such as existence, threshold, or Boolean, the corresponding tables (existence, threshold, and Boolean tables) are populated with the information required to perform the test. You can set event triggers based on existence, threshold, and Boolean trigger types.

The existence trigger tests are performed based on the following parameters:

- Absent
- Present
- Changed

The Boolean tests are comparison tests that are performed based on one of the following parameters:

- Unequal
- Equal
- Less
- Less Or Equal
- Greater
- Greater Or Equal

The threshold tests are performed based on the following parameters:

- Rising
- Falling
- Rising or Falling

## Examples

The following example shows how to enable the existence trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test existence
Router(config-event-trigger-existence)#
```

The following example shows how to enable the Boolean trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name EventA
Router(config-event-trigger)# test boolean
Router(config-event-trigger-boolean)#
```

The following example shows how to enable the threshold trigger test:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test threshold
Router(config-event-trigger-threshold)#
```

## Related Commands

Command	Description
<b>comparison</b>	Specifies the type of Boolean test comparison to perform.
<b>event owner</b>	Specifies an owner for event trigger.
<b>object list owner</b>	Specifies an owner for the list of objects configured for an event.
<b>startup</b>	Specifies whether an event can be triggered during a trigger test.
<b>value</b>	Sets a value to the object.

# test snmp trap config-copy

To verify the reception of config-copy notifications by the Network Management System (NMS) or the Simple Network Management Protocol (SNMP) manager in a simulated scenario, use the **test snmp trap config-copy** command in privileged EXEC mode.

## test snmp trap config-copy

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

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	12.2(33)SXI	This command was introduced.
	12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

**Usage Guidelines** The Config-Copy MIB facilitates the copying of SNMP agent configuration files to the startup configuration or the local Cisco IOS file system, and vice versa. The config-copy notifications are sent to the NMS or the SNMP manager to indicate the successful completion of config-copy operation to or from the SNMP agent.

**Examples** The following example shows how to simulate the verification of config-copy traps:

```
Router# test snmp trap config-copy

Generating CONFIG-COPY-MIB trap

00:20:44: SNMP: Queuing packet to 10.2.14.2
00:20:44: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 124470
snmpTrapOID.0 = ccCopyMIBTraps.1
ccCopyTable.1.5.2 = 10.10.10.10
ccCopyTable.1.6.2 =
ccCopyTable.1.10.2 = 3
ccCopyTable.1.11.2 = 124470
ccCopyTable.1.12.2 = 124470
Router#
```

Related Commands	Command	Description
	<b>debug snmp packet</b>	Displays information about every SNMP packet sent or received by the router.
	<b>snmp-server enable traps</b>	Enables all SNMP notification types that are available on your system.
	<b>snmp-server host</b>	Specifies the recipient of an SNMP notification operation.

# test snmp trap snmp

To verify the reception of Simple Network Management Protocol (SNMP) notifications by the Network Management System (NMS) or the SNMP manager in a simulated scenario, use the **test snmp trap snmp** command in privileged EXEC mode.

**test snmp trap snmp {authentication | coldstart | linkup | linkdown | warmstart}**

Syntax Description		
	<b>authentication</b>	Verifies the generation and reception of the SNMP authentication failure notification by the SNMP manager. The authentication failure trap indicates that the SNMP agent has received a protocol message from the SNMP manager that is not properly authenticated.
	<b>coldstart</b>	Verifies the generation and reception of the SNMP coldStart notifications by the SNMP manager. A coldStart trap indicates that the SNMP agent is reinitializing and its configuration may have changed.
	<b>linkup</b>	Verifies the generation and reception of the SNMP linkUp notifications by the SNMP manager. A linkUp trap indicates if a communication link represented in the agent's configuration is activated.
	<b>linkdown</b>	Verifies the generation and reception of the SNMP linkDown notifications by the SNMP manager. A linkDown trap indicates if a communication link represented in the agent's configuration fails.
	<b>warmstart</b>	Verifies the generation and reception of the SNMP warmStart notifications by the SNMP manager. A warmStart trap indicates that the SNMP agent is reinitializing and its configuration is not modified.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	12.2(33)SXI	This command was introduced.
	12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

**Usage Guidelines** SNMP traps or notifications provide information about improper user authentication, restarts, closing of a connection, loss of connection to a neighbor router, or other significant events to the NMS.

Before testing the SNMP traps, configure the SNMP manager for the device and enable SNMP traps.

**Examples** The following example shows how to simulate the verification of the authentication failure trap:

```
Router# test snmp trap snmp authentication
```

```
Generating Authentication failure trap
```

```
Sep 12 08:37:49.935: SNMP: Queuing packet to 10.4.9.2
```

```
Sep 12 08:37:49.935: SNMP: V1 Trap, ent snmpTraps, addr 192.168.0.1, gentrap 4  
lssystem.5.0 = 10.10.10.10
```

```
ciscoMgmt.412.1.1.1.0 = 1
ciscoMgmt.412.1.1.2.0 = 10.10.10.10
Sep 12 08:38:55.995: SNMP: Packet sent via UDP to 10.4.9.2
Sep 12 08:38:56.263: SNMP: Packet sent via UDP to 10.4.9.2
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug snmp packet</b>	Displays information about every SNMP packet sent or received by the router.
<b>snmp-server enable traps</b>	Enables all SNMP notification types that are available on your system.
<b>snmp-server host</b>	Specifies the recipient of an SNMP notification operation.

# test snmp trap syslog

To verify the reception of the system logging message Simple Network Management Protocol (SNMP) notifications by the SNMP manager in a simulated scenario, use the **test snmp trap syslog** command in privileged EXEC mode.

## test snmp trap syslog

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

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	12.2(33)SX1	This command was introduced.
	12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

**Usage Guidelines** System logging messages are status notification messages that are generated by the routing device during operation. These messages are typically logged to a destination such as the terminal screen, or to a remote syslog host.

**Examples** The following example shows how to replicate a syslog trap and its reception by the NMS:

```
Router# test snmp trap syslog

Generating SYSLOG-MIB Trap

00:07:25: SNMP: Queuing packet to 10.4.9.2
00:07:25: SNMP: V1 Trap, ent ciscoSyslogMIB.2, addr 192.16.12.8, gentrap 6, spectra
  clogHistoryEntry.2.1 = TEST
  clogHistoryEntry.3.1 = 5
  clogHistoryEntry.4.1 = 1.3.6.1.4.1.9.9.10.1
  clogHistoryEntry.5.1 = Syslog test trap
  clogHistoryEntry.6.1 = 44596
00:07:25: SNMP: Queuing packet to 10.4.9.2
00:07:25: SNMP: V2 Trap, reqid 4, errstat 0, erridx 0
  sysUpTime.0 = 44596
  snmpTrapOID.0 = ciscoSyslogMIB.2.0.1
  clogHistoryEntry.2.1 = TEST
  clogHistoryEntry.3.1 = 5
  clogHistoryEntry.4.1 = 1.3.6.1.4.1.9.9.10.1
  clogHistoryEntry.5.1 = Syslog test trap
  clogHistoryEntry.6.1 = 44596
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug snmp packet</b>	Displays information about every SNMP packet sent or received by the router.
<b>snmp-server enable traps</b>	Enables all SNMP notification types that are available on your system.
<b>snmp-server host</b>	Specifies the recipient of an SNMP notification operation.

# time-period

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

**time-period** *minutes*

**no time-period** *minutes*

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

<b>Command Default</b>	By default, no time increment is set.
------------------------	---------------------------------------

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

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

## Usage Guidelines



### Note

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

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



### Note

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

**Examples**

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

```
Router# configure terminal
!
Router(config)# archive
Router(config-archive)# path disk0:myconfig
Router(config-archive)# time-period 20
Router(config-archive)# end
```

**Related Commands**

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

# time-range

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

**time-range** *time-range-name*

**no time-range** *time-range-name*

## Syntax Description

*time-range-name* Desired name for the time range. The name cannot contain either a space or quotation mark, and it must begin with a letter.

## Command Default

None

## Command Modes

Global configuration  
Webvpn context configuration

## Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(17a)SX	Support for this command was implemented on the Cisco 7600 series routers.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was available in webvpn context configuration mode.

## Usage Guidelines

The **time-range** entries are identified by a name, which is referred to by one or more other configuration commands. Multiple time ranges can occur in a single access list or other feature.



### Note

In Cisco IOS 12.2SX releases, IP and IPX-extended access lists are the only types of access lists that can use time ranges.

After the **time-range** command, use the **periodic** time-range configuration command, the **absolute** time-range configuration command, or some combination of them to define when the feature is in effect. Multiple **periodic** commands are allowed in a time range; only one **absolute** command is allowed.



### Tip

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

**Examples**

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

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

**Related Commands**

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

# track stub

To create a stub object that can be tracked by Embedded Event Manager (EEM) and to enter tracking configuration mode, use the **track stub** command in global configuration mode. To remove the stub object, use the **no** form of this command.

**track** *object-number* **stub**

**no track** *object-number* **stub**

<b>Syntax Description</b>	<i>object-number</i>	Object number that represents the object to be tracked. The range is from 1 to 500.
---------------------------	----------------------	---

<b>Command Default</b>	No stub objects are created.
------------------------	------------------------------

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(2)T	This command was introduced.
	12.2(31)SB3	This command was integrated into Cisco IOS Release 12.2(31)SB3.
	12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
	Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
	12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

<b>Usage Guidelines</b>	Use the <b>track stub</b> command to create a stub object, which is an object that can be tracked and manipulated by an external process, EEM. After the stub object is created, the <b>default-state</b> command can be used to set the default state of the stub object.
-------------------------	--

EEM is a distributed, scalable, and customized approach to event detection and recovery offered directly in a Cisco IOS device. EEM offers the ability to monitor events and take informational or corrective action when the monitored events occur or when a threshold is reached. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs.

<b>Examples</b>	In the following example, stub object 1 is created and configured with a default state of up.
-----------------	---

```
track 1 stub
default-state up
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>default-state</b>	Sets the default state for a stub object.
<b>show track</b>	Displays tracking information.

# transfer-interval

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

**transfer-interval** *minutes*

**no transfer-interval**

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

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

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release XE 2.1.

**Usage Guidelines** Bulk statistics data is collected into a new file when a transfer attempt begins, which means that this command also configures the collection interval.

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

**Examples** The following example shows how to configure a transfer interval of 20 minutes for the bulk statistics configuration bulkstat1:

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

---

**Related Commands**

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

## transport (WSMA)

To define a transport configuration for a Web Services Management Agent (WSMA) profile, use the **transport** command in WSMA listener configuration mode. To disable the transport configuration, use the **no** form of this command.

```
transport { ssh subsys subsys-name | http path path-name | https path path-name }
```

```
no transport
```

Syntax Description		
<b>ssh</b>		Enables the WSMA profile to listen on the Secure Shell Version 2 (SSHv2) port.
<b>subsys</b>		Defines the SSH subsystem to use.
<i>subsys-name</i>		Defines a name for the SSH subsystem. By default, wsma is used as the subsystem name.
<b>http</b>		Enables the WSMA profile to listen on the HTTP port.
<b>path</b>		Defines the HTTP path to use.
<i>path-name</i>		Defines a path name for the HTTP or HTTPS path. The path-name must begin with a /. By default, /wsma is used as the path-name.
<b>https</b>		Enables the WSMA profile to listen on the HTTPS port.

**Command Default** The transport is not configured.

**Command Modes** WSMA listener configuration (config-wsma-listen)

**Usage Guidelines** You can use the **transport** command to define the transport termination points for a WSMA profile. Defining the transport configuration leads to the opening of a listening socket for listeners on the router or connecting sockets for clients on the router. Opening the listening sockets enables the WSMA to start listening to messages.

SSHv2, HTTP, and HTTPS are the types of transport configuration available for a WSMA profile.

Use this command from the WSMA listener configuration mode. To enter this mode, enter the **wsma profile listener** command in global configuration mode.

**Examples** The following example shows how to use the SSHv2 protocol to enable the listener profile:

```
Router (config)# wsma profile listener prof1
Router (config-wsma-listen)# transport ssh subsys wsma
Router (config-wsma-listen)#
```

Command History	Release	Modification
	12.4(24)T	This command was introduced.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>acl</b>	Enables access control lists for restricting addresses that can connect to a WSMA profile.
<b>encap</b>	Configures an encapsulation for a WSMA profile.
<b>idle-timeout</b>	Sets a time for the WSMA profile to disconnect the session when there is no network traffic.
<b>max-message</b>	Sets the maximum size limit for incoming messages.
<b>stealth</b>	Disables WSMA from sending SOAP faults.
<b>wsma profile listener</b>	Configures and enables a WSMA listener profile.
<b>wsse</b>	Enables the WSSE for a WSMA profile.

# transport event

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

**transport event**

**no transport event**

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

**Defaults** Disabled

**Command Modes** CNS inventory configuration

Command History	Release	Modification
	12.3(1)	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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

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

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

Related Commands	Command	Description
	<b>cns inventory</b>	Enables the CNS inventory agent and enters CNS inventory configuration mode.

# trigger (EEM)

To enter trigger applet configuration mode and specify the multiple event configuration statements for an Embedded Event Manager (EEM) applet, use the **trigger** command in applet configuration mode. To disable the multiple event configuration statements, use the **no** form of this command.

**trigger** [**occurs** *occurs-value*] [**period** *period-value*] [**period-start** *period-start-value*] [**delay** *delay-value*]

**no trigger** [**occurs** *occurs-value*] [**period** *period-value*] [**period-start** *period-start-value*] [**delay** *delay-value*]

## Syntax Description

<b>occurs</b>	(Optional) Specifies the number of times the total correlation occurs before an EEM event is raised. When a number is not specified, an EEM event is raised on the first occurrence.
<i>occurs-value</i>	(Optional) Number in the range from 1 to 4294967295.
<b>period</b>	(Optional) Specifies the time interval during which the one or more occurrences must take place. If not specified, the time-period check is not applied.
<i>period-value</i>	(Optional) Number that represents seconds and optional milliseconds in the format <i>sssssssss[.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> .
<b>period-start</b>	(Optional) Specifies the start of an event correlation window. If not specified, event monitoring is enabled after the first CRON period occurs.
<i>period-start-value</i>	(Optional) String that specifies the beginning of an event correlation window.
<b>delay</b>	(Optional) Specifies the number of seconds after which an event will be raised if all the conditions are true. If not specified, the event will be raised immediately.
<i>delay-value</i>	(Optional) Number that represents seconds and optional milliseconds in the format <i>sssssssss[.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> .

## Command Default

Disabled.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

**Usage Guidelines**

The **trigger** command relates multiple event statements using the optional **tag** keyword with the *event-tag* argument specified in each event statement.

**Examples**

The following example shows how to use the **trigger** command to enter trigger applet configuration mode and specify multiple event configuration statements for an EEM applet. In this example, the applet is run when the **show bgp all** command and any syslog message that contains the string "COUNT" occurs within a period of 60 seconds.

```
Router(config)# event manager applet delay_50
Router(config-applet)# event tag 1.0 cli pattern "show bgp all" sync yes occurs 32 period
60 maxrun 60
Router(config-applet)# event tag 2.0 syslog pattern "COUNT"
Router(config-applet)# trigger occurs 1 delay 50
Router(config-applet-trigger)# correlate event 1.0 or event 2.0
Router(config-applet-trigger)# attribute tag 1.0 occurs 1
Router(config-applet-trigger)# attribute tag 2.0 occurs 1
Router(config-applet-trigger)# action 1.0 cli command "show memory"
Router(config-applet)# action 2.0 cli command "enable"
Router(config-applet)# action 3.0 cli command "config terminal"
Router(config-applet)# action 4.0 cli command " ip route 192.0.2.0 255.255.255.224
192.0.2.12"
Router(config-applet)# action 91.0 cli command "exit"
Router(config-applet)# action 99.0 cli command "show ip route | incl 192.0.2.5"
```

**Related Commands**

Command	Description
<b>attribute (EEM)</b>	Specifies a complex event for an EEM applet.
<b>correlate</b>	Builds a single complex event.
<b>event manager applet</b>	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

# tll dns

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

**tll dns** *seconds*

**no tll dns** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Integer in the range from 10 to 2147483647 that specifies the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.
---------------------------	----------------	--

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

**Command Modes** Boomerang configuration

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

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

The **tll dns** command configures the number of seconds for which the DNS client can cache a boomerang reply from a boomerang client.

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

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

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>alias (boomerang configuration)</b>	Configures an alias name for a specified domain.
<b>ip drp domain</b>	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.
<b>server (boomerang configuration)</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>ttl 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.

# tll ip

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

**tll ip** *hops*

**no tll ip** *hops*

## Syntax Description

<i>hops</i>	Integer in the range from 1 to 255 that specifies the number of hops that occur between the boomerang client and the DNS client before the boomerang response packet fails.
-------------	---

## Command Default

No default behavior or values.

## Command Modes

Boomerang configuration

## Command History

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

## Usage Guidelines

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

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

## Examples

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

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

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>alias (boomerang)</b>	Configures an alias name for a specified domain.
<b>ip drp domain</b>	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.
<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>ttl dns</b>	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.

# type (test existence)

To specify the type of existence trigger test to perform, use the **type** command in event trigger existence configuration mode. To disable the specified trigger test type, use the **no** form of this command.

**type** { **present** | **absent** | **changed** }

**no type** { **present** | **absent** | **changed** }

Syntax Description		
	<b>present</b>	Specifies whether the trigger conditions for the existence test are present.
	<b>absent</b>	Specifies whether the trigger conditions for the existence test are absent.
	<b>changed</b>	Specifies whether the trigger conditions for the existence test are changed.

**Command Default** By default, both present and absent tests are performed.

**Command Modes** Event trigger existence configuration (config-event-trigger-existence)

Command History	Release	Modification
	12.4(20)T	This command was introduced.
	12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

**Usage Guidelines** The existence trigger tests are performed based on the following parameters:

- Absent
- Present
- Changed

When the test type is not specified, both present and absent tests are performed.

**Examples** The following example shows how to specify the existence trigger test as present:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test existence
Router(config-event-trigger-existence)# type present
Router(config-event-trigger-existence)#
```

Related Commands	Command	Description
	<b>test</b>	Enables a trigger test.

## url (bulkstat)

To specify the host to which bulk statistics files should be transferred, use the **url** command in Bulk Statistics Transfer configuration mode. To remove a previously configured destination host, use the **no** form of this command.

```
url {primary | secondary} url
```

```
no url {primary | secondary}
```

Syntax Description	primary	secondary
	Specifies the URL to be used first for bulk statistics transfer attempts.	Specifies the URL to be used for bulk statistics transfer attempts if the transfer to the primary URL is not successful.
	<i>url</i>	
	Destination URL address for the bulk statistics file transfer. Use FTP, RCP, or TFTP. The Cisco IOS File System (IFS) syntax for these URLs is as follows:	
	<ul style="list-style-type: none"> <li>• <b>ftp:</b>[[[/username [:password]@]location]/directory]/filename</li> <li>• <b>rnp:</b>[[[/username@]location]/directory]/filename</li> <li>• <b>tftp:</b>[[/location]/directory]/filename</li> </ul>	
	The <i>location</i> argument is typically an IP address.	

**Command Default** No host is specified.

**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.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release XE 2.1.

**Usage Guidelines** For bulk statistics transfer retry attempts, a single retry consists of an attempt to send first to the primary URL, and then to the secondary URL.

**Examples**

In the following example, an FTP server is used as the primary destination for the bulk statistics file. If a transfer to that address fails, an attempt is made to send the file to the TFTP server at 192.168.10.5. No retry command is specified, which means that only one attempt to each destination will be made.

```
Router(config)# snmp mib bulkstat transfer ifMibTesting
Router(config-bulk-tr)# schema carMibTesting1
Router(config-bulk-tr)# schema carMibTesting2
Router(config-bulk-tr)# format bulkBinary
Router(config-bulk-tr)# transfer-interval 60
Router(config-bulk-tr)# buffer-size 10000
Router(config-bulk-tr)# url primary ftp://user2:pswd@192.168.10.5/functionality/
Router(config-bulk-tr)# url secondary tftp://user2@192.168.10.8/tftpboot/
Router(config-bulk-tr)# buffer-size 2500000
Router(config-bulk-tr)# enable
Router(config-bulk-tr)# exit
```

**Related Commands**

Command	Description
<b>retry (bulkstat)</b>	Configures the number of retries that should be attempted for sending bulk statistics files.
<b>snmp mib bulkstat transfer</b>	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.

## user (ERM)

To apply a global policy, create a resource group, or add resource users (RUs) to a resource group, use the **user** command in Embedded Resource Manager (ERM) configuration mode. To disable applying the policy, use the **no** form of this command.

```
user { resource-instance-name resource-user-type resource-policy-name | global
global-policy-name | group resource-group-name type resource-user-type }
```

```
no user { resource-instance-name resource-user-type resource-policy-name | global
global-policy-name | group resource-group-name type resource-user-type }
```

### Syntax Description

<i>resource-instance-name</i>	Name of the RU to which you are applying a policy.
<i>resource-user-type</i>	Name of the RU type.
<i>resource-policy-name</i>	Name of the policy you are applying to the specified RU.
<b>global</b>	Applies a global policy.
<i>global-policy-name</i>	Name of the global policy you are applying.
<b>group</b>	Specifies a resource group to which the policy is being applied.
<i>resource-group-name</i>	Name of the resource group to which the policy is being applied.
<b>type</b>	Specifies the type of the RU to which the policy is being applied.
<i>resource-user-type</i>	Name of the RU type to which the policy is being applied.

### Command Default

No policy is configured.

### Command Modes

ERM configuration (config-erm)

### Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

### Usage Guidelines

This command helps you to apply the various policies (system global, per-user local, and user global) to resource owners (ROs), RUs, or a group of RUs.

Use the **user** *resource-instance-name* *resource-user-type* *resource-policy-name* command to apply a specified policy to a RU. This policy is also known as a per-user local policy or per-user template.

Use the **user global** *global-policy-name* command to apply a global thresholding policy to all the users.

Use the **user group** *resource-group-name* **type** *resource-user-type* command to create a resource group and to enter resource group configuration mode. After you create the resource group, you can add RUs using the **instance** *instance-name* command and apply the same thresholding policy to all the RUs against the resource group using the **policy** *policy-name* command in resource group configuration mode.

For example, you created a resource group named `lowPrioUsers` with a type of `iosprocess`. You have low-priority RUs or tasks such as HTTP and Simple Network Management Protocol (SNMP), and you want to set a threshold for all the low-priority RUs as a group. 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 apply sets a minor rising threshold value of 10 percent for the resource group, when the accumulated usage of both HTTP and SNMP RUs crosses the 10 percent mark, a notification is sent to the RUs in the resource group `lowPrioUsers`. That is, if HTTP usage is 4 percent and SNMP usage is 7 percent, a notification is sent to `lowPrioUsers`.

## Examples

The following example shows how to apply a per-user thresholding policy for the resource instance EXEC, resource user type `iosprocess`, and resource policy name `policy-test1`:

```
Router(config-erm) # user EXEC iosprocess policy-test1
```

The following example shows how to apply a global thresholding policy with policy name `global-global-test1`:

```
Router(config-erm) # user global global-global-test1
```

The following example shows how to create a resource group with the resource group name `lowPrioUsers` and RU type as `iosprocess`, and how to add the RU HTTP to the resource group and apply a thresholding policy `group-policy1`:

```
Router(config-erm) # user group lowPrioUsers type iosprocess
Router(config-res-group) # instance http
Router(config-res-group) # policy group-policy1
```

## Related Commands

Command	Description
<b>instance (resource group)</b>	Adds RUs to a resource group.
<b>policy (ERM)</b>	Configures an ERM resource policy.
<b>policy (resource group)</b>	Applies the same policy to all the RUs in a resource group.
<b>resource policy</b>	Enters ERM configuration mode.
<b>show resource all</b>	Displays resource details for all RUs.

## value (action set)

To set a value to the object, use the **value** command in event action set configuration mode. To disable the configured settings, use the **no** form of this command.

**value** *integer-value*

**no value**

<b>Syntax Description</b>	<i>integer-value</i>	Numerical value to set for the object.
---------------------------	----------------------	--

<b>Command Default</b>	By default, no value is set for the object.
------------------------	---

<b>Command Modes</b>	Event action set configuration (config-event-action-set)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.	

<b>Usage Guidelines</b>	The <b>value</b> command sets the value for the object associated with the event for which actions are set by using the <b>action set</b> command.
-------------------------	--

<b>Examples</b>	The following example shows how to set a value of 2 to the object:
-----------------	--

```
Router(config)# snmp mib event owner owner1 name EventA
Router(config-event)# action set
Router(config-event-action-set)# value 2
Router(config-event-action-set)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>action</b>	Sets an action for an event.

## value (test boolean)

To set a value for the Boolean trigger test, use the **value** command in event trigger boolean configuration mode. To disable the configured settings, use the **no** form of this command.

**value** *integer-value*

**no value**

<b>Syntax Description</b>	<i>integer-value</i>	Numerical value to set for the Boolean test. The default is 0.
---------------------------	----------------------	--

<b>Command Default</b>	The Boolean trigger test value is set to 0.
------------------------	---

<b>Command Modes</b>	Event trigger boolean configuration (config-event-trigger-boolean)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.	

<b>Usage Guidelines</b>	The <b>value</b> command specifies the value to set for the Boolean trigger test.
-------------------------	---

<b>Examples</b>	The following example shows how to set a value for the Boolean trigger test:
-----------------	--

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test boolean
Router(config-event-trigger-boolean)# value 10
Router(config-event-trigger-boolean)
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>test</b>	Enables a trigger test.

# value type

To specify the type of expression to use during object sampling, use the **value type** command in expression configuration mode. To disable the specified value type, use the **no** form of this command.

**value type** { **counter32** | **unsigned32** | **timeticks** | **integer32** | **ipaddress** | **octetstring** | **objectid** | **counter64** }

**no value type**

Syntax Description	
<b>counter32</b>	(Optional) Specifies a counter32 value. Counter32 specifies a value that represents a count. The value ranges from 0 to 4294967295.
<b>unsigned32</b>	(Optional) Specifies an unsigned integer value. Unsigned32 specifies a value that includes only non-negative integers. The value ranges from 0 to 4294967295.
<b>timeticks</b>	(Optional) Specifies a value based on timeticks. Timeticks represents a non-negative integer value that specifies the elapsed time between two events, in units of hundredth of a second.  When objects in the MIB are defined using the subset of Abstract Syntax Notation One (ASN.1), the description of the object type identifies this reference period.
<b>integer32</b>	(Optional) Specifies an integer32 value. The Integer32 represents 32-bit signed integer values for Simple Network Management Protocol (SNMP). The value range includes both negative and positive numbers.
<b>ipaddress</b>	(Optional) Specifies a value based on the IP address. The IP address is a string of four octets. The IP address value type is generally an IPv4 address. This value is encoded as four bytes in the network byte order.
<b>octetstring</b>	(Optional) Specifies a value based on octetstring. The octetstring specifies octets of binary or textual information. The octet string length ranges from 0 to 65535 octets.
<b>objectid</b>	(Optional) Specifies a value based on the object identifier of an object. Each object type in a MIB is identified by an object identifier value assigned by the administrator. The object identifier identifies the value type that has an assigned object identifier value.
<b>counter64</b>	(Optional) Specifies a counter64 value. Counter64, like counter32, specifies a value that represents a count. However, the counter64 value ranges from 0 to 18446744073709551615. This value type is used when a 32-bit counter rollover occurs in less than an hour.

**Command Default** The default value type is counter32.

**Command Modes** Expression configuration mode (config-expression)

**Command History**

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

**Usage Guidelines**

The **value type** command specifies a value for expression evaluation.

**Examples**

The following example shows how to specify the counter32 value type:

```
Router(config)# snmp mib expression owner owner1 name ExpressionA
Router(config-expression)# value type counter32
Router(config-expression)#
```

**Related Commands**

Command	Description
<b>snmp mib expression owner</b>	Specifies the owner for an expression.

# wildcard

To specify whether the object identifier needs to be wildcarded, use the **wildcard** command in event object list, event action set, or expression object configuration mode. To disable the configured settings, use the **no** form of this command.

**wildcard**

**no wildcard**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Objects are fully specified by default.

## Command Modes

Event object list configuration (config-event-objlist)  
 Event action set configuration (config-action-set)  
 Expression object configuration (config-expression-object)

## Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

## Usage Guidelines

The **wildcard** indicates whether an object identifier needs to be wildcarded or fully specified. By default, the objects are based on instances and are not wildcarded.

## Examples

The following example shows how to specify wildcard for an object instance during object list configuration:

```
Router(config)# snmp mib event object list owner owner1 name objectA 10
Router(config-event-objlist)# wildcard
Router(config-event-objlist)#
```

The following example shows how to specify wildcard for an object instance during action set configuration:

```
Router(config)# snmp mib event owner owner1 name EventA
Router(config-event)# action set
Router(config-event-action-set)# wildcard
Router(config-event-action-set)#
```

The following example shows how to specify wildcard for an object instance during expression configuration:

```
Router(config)# snmp mib expression owner owner1 name ExpressionA
Router(config-expression)# object 10
Router(config-expression-object)# wildcard
```

```
Router (config-expression-object) #
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>object id</b>	Specifies the object identifier of an object.
<b>snmp mib event object list</b>	Configures a list of objects for events, event triggers, and trigger tests.
<b>snmp mib expression owner</b>	Specifies the owner for an expression.

# write mib-data

To save MIB data to system memory (NVRAM) for MIB Data Persistence, use the **write mib-data** command in EXEC mode.

## write mib-data

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

**Command Modes** Exec

Command History	Release	Modification
	12.2(2)T	This command was introduced as part of the “Circuit Interface Identification Persistence for SNMP” feature.
	12.2(4)T	MIB Data Persistence for the Event and Expression MIBs was introduced as part of the “Distributed Management Event and Expression MIB Persistence” feature.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

**Usage Guidelines** The MIB Data Persistence feature allows the SNMP data of a MIB to be persistent across reloads; that is, the values of certain MIB objects are retained even if your networking device reboots.

To determine which MIBs support “MIB Persistence” in your release, use the **snmp mib persist ?** command in global configuration mode.

Any modified MIB data must be written to NVRAM memory using the **write mib-data** command. If the **write mib-data** command is not used, modified MIB data is not saved automatically, even if MIB Persistence is enabled. Executing the **write mib-data** command saves only the current MIB data; if the MIB object values are changed, you should reenter the **write mib-data** command to ensure that those values are persistent across reboots.

**Examples** In the following example, Event MIB Persistence and Circuit MIB persistence are enabled, and any currently set object values for those MIBs are saved to NVRAM:

```
Router# configure terminal
Router(config)# snmp mib persist circuit
Router(config)# snmp mib persist event
Router(config)# end
Router# write mib-data
```

Related Commands	Command	Description
	<b>snmp mib persist</b>	Enables MIB data persistence.

# wsma agent

To enable a specific Web Services Management Agent (WSMA) and associate it with a profile, use the **wsma agent** command in global configuration mode. To disable the WSMA agent and its associations with a profile, use the **no** form of this command.

```
wsma agent { config | exec | fileSYS | notify } profile profile-name
```

```
no wsma agent { config | exec | fileSYS | notify }
```

## Syntax Description

<b>config</b>	Starts the WSMA config agent.
<b>exec</b>	Starts the WSMA exec agent.
<b>fileSYS</b>	Starts the WSMA fileSYS agent.
<b>notify</b>	Starts the WSMA notify agent.
<b>profile</b> <i>profile-name</i>	Defines the profile name to use.

## Command Default

By default, WSMA agents are disabled and are not associated with profiles.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.4(24)T	This command was introduced.

## Examples

The following example shows how to enable a WSMA agent and associate with a profile:

```
Router(config)# wsma agent config profile wsmal
Router(config)#
```

## Related Commands

Command	Description
<b>wsma id</b>	Assigns unique WSMA IDs to Cisco IOS devices.
<b>wsma profile listener</b>	Configures and enables a WSMA listener profile.

# wsma id

To assign unique Web Services Management Agent (WSMA) IDs to IOS devices, use the **wsma id** command in global configuration mode. To disable the WSMA IDs assigned to Cisco IOS devices, use the **no** form of this command.

```
wsma id { hardware-serial | hostname | ip-address interface-type | mac-address interface-type |
string value }
```

```
no wsma id
```

## Syntax Description

<b>hardware-serial</b>	Assigns the hardware serial number as a unique ID.
<b>hostname</b>	Assigns the host name as a unique ID.
<b>ip-address</b>	Assigns the IP address of the specified interface as unique ID.
<i>interface-type</i>	Specifies the interface type.
<b>mac-address</b>	Assigns the IP address of the specified interface as unique ID.
<b>string value</b>	Defines a string value to be assigned as unique ID.

## Command Default

By default, unique WSMA IDs are not assigned to Cisco IOS devices.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.4(24)T	This command was introduced.

## Usage Guidelines

Use this command to assign unique IDs to Cisco IOS devices. Unique IDs can also be configured by specifying required parameters.

Whenever the WSMA ID changes, all WSMA sessions are terminated. This is done in order to protect the management applications from not having to deal with synchronizing states dynamically.

## Examples

The following example shows how to assign WSMA IDs:

```
Router(config)# wsma id ip-address fastethernet 0/1
Router(config)#
```

## Related Commands

Command	Description
<b>wsma agent</b>	Enables a specific WSMA and associates it with a profile.
<b>wsma profile listener</b>	Configures and enables a WSMA listener profile.

# wsma profile listener

To configure and enable a Web Services Management Agent (WSMA) listener profile and to enter WSMA listener configuration mode, use the **wsma profile listener** command in global configuration mode. To disable a WSMA listener profile, use the **no** form of this command.

**wsma profile listener** *profile-name*

**no wsma profile listener** *profile-name*

## Syntax Description

<b>listener</b>	Enables the WSMA listener profile for the specified profile name.
<i>profile-name</i>	Defines the name of the listener profile to be enabled.

## Command Default

No WSMA profiles are configured.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.4(24)T	This command was introduced.

## Usage Guidelines

You can use the **wsma profile listener** command to configure and enable a WSMA profile. A WSMA profile associated with a specific WSMA constitutes an operational embedded agent.

WSMA profiles work as a transport termination point, and allows transport and XML encapsulation parameters to be configured.

- The configurable encapsulations for WSMA are SOAP 1.1 and SOAP 1.2.
- The transportation mechanism for WSMA includes SSH, HTTP, and HTTPS. These encapsulations open listening sockets for listeners on the router or connecting sockets for clients on the router.

The **wsma profile listener** command creates a passive listening socket on the Cisco IOS device. It receives incoming messages provided they match the configured ACL requirements. You can configure various parameters for a WSMA profile in WSMA listener configuration mode.

## Examples

The following example shows how to enable a WSMA listener profile:

```
Router(config)# wsma profile listener prof1
Router(config-wsma-listen)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>acl</b>	Enables access control lists for restricting addresses that can connect to a WSMA profile.
<b>encap</b>	Configures an encapsulation for a WSMA profile.
<b>idle-timeout</b>	Sets a time for the WSMA profile to disconnect the session when there is no network traffic.
<b>transport</b>	Defines a transport configuration for a WSMA profile.
<b>max-message</b>	Sets the maximum size limit for incoming messages.
<b>stealth</b>	Disables WSMA from sending SOAP faults.
<b>wsma agent</b>	Enables a specific WSMA and associates it with a profile.
<b>wsma id</b>	Assigns unique WSMA IDs to Cisco IOS networking devices.
<b>wsse</b>	Enables the WSSE for a WSMA profile.

## WSSE

To enable the Web Services Security Header (WSSE) for a Web Services Management Agent (WSMA), use the **wsse** command in WSMA listener configuration mode. To disable the security header, use the **no** form of this command.

**wsse**

**no wsse**

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

**Command Default** WSSE is enabled.

**Command Modes** WSMA listener configuration (config-wsma-listen)

### Command History

Release	Modification
12.4(24)T	This command was introduced.

### Usage Guidelines

You can use the **wsse** command to enable the WSSE for a WSMA profile. When enabled, the WSSE username and password are required in the SOAP header. By default, this command is enabled and the nonvolatile generation (NVGEN) operation does not take place. Specifying the **no wsse** command enables the NVGEN operation.

Use this command from the WSMA listener configuration mode. To enter this mode, enter the **wsma profile listener** command in global configuration mode.

### Examples

The following example shows how to enable WSSE on a WSMA profile:

```
Router(config)# wsma profile listener prof1
Router(config-wsma-listen)# wsse
Router(config-wsma-listen)#
```

### Related Commands

Command	Description
<b>acl</b>	Enables access control lists for restricting addresses that can connect to a WSMA profile.
<b>encap</b>	Configures an encapsulation for a WSMA profile.
<b>idle-timeout</b>	Sets a time for the WSMA profile to disconnect the session when there is no network traffic.
<b>max-message</b>	Sets the maximum size limit for incoming messages.
<b>stealth</b>	Disables WSMA from sending SOAP faults.

<b>Command</b>	<b>Description</b>
<b>transport</b>	Defines a transport configuration for a WSMA profile.
<b>wsma profile listener</b>	Configures and enables a WSMA listener profile.

# xsm

To enable XML Subscription Manager (XSM) client access to the device, use the **xsm** command in global configuration mode. To disable XSM client access to the device, use the **no** form of this command.

**xsm**

**no xsm**

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

**Command Default** XSM client access to the device is enabled.

**Command Modes** Global configuration

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

**Usage Guidelines** This command requires that the **ip http server** command is enabled. Enabling the **xsm** command also enables the **xsm vdm** and **xsm edm** commands. This command must be enabled for the XSM client (such as VPN Device Manager [VDM]) to operate.

**Examples** In the following example, access by remote XSM clients to XSM data on the device is disabled:

```
Router# no xsm
```

Command	Description
<b>ip http server</b>	Enables a device to be reconfigured through the Cisco browser interface.
<b>show xsm status</b>	Displays information and status about clients subscribed to the XSM server.
<b>show xsm xrd-list</b>	Displays all XRDs for clients subscribed to the XSM server.
<b>xsm dvdm</b>	Grants access to switch operations.

<b>Command</b>	<b>Description</b>
<b>xsm edm</b>	Grants access to EDM monitoring and configuration data.
<b>xsm vdm</b>	Grants access to VPN-specific monitoring and configuration data.

# xsm dvdm

To enable switch-specific configuration data (for example, configuring switch ports and VLANs) when running VPN Device Manager (VDM) on a switch, use the **xsm dvdm** command in global configuration mode. To disable switch-specific configuration data for VDM, use the **no** form of this command.

**xsm dvdm**

**no xsm dvdm**

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

**Command Default** Access to switch-specific configuration data is enabled when XSM is enabled.

**Command Modes** Global configuration

## Command History

Release	Modification
12.2(9)Y01	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

## Usage Guidelines

Access to switch-specific configuration data (dVDM) is enabled by default when XSM is enabled.

The **no xsm dvdm** command allows you to disable only switch-specific XSM data. Note however that disabling dVDM will prevent the VDM application from communicating properly with the device (switch). There is minimal performance impact associated with leaving dVDM enabled.

## Examples

In the following example, access to switch-specific configuration data is disabled in XSM:

```
Router(config)# no xsm dvdm
```

## Related Commands

Command	Description
<b>xsm</b>	Enables XSM client access to the router.
<b>xsm edm</b>	Grants access to EDM monitoring and configuration data.
<b>xsm history vdm</b>	Enables specific VPN statistics collection on the XSM server.
<b>xsm vdm</b>	Grants access to VPN-specific monitoring and configuration data.

# xsm edm

To grant access to Embedded Device Manager (EDM) monitoring and configuration data, use the **xsm edm** command in global configuration mode. To cancel access to EDM monitoring and configuration data, use the **no** form of this command.

**xsm edm**

**no xsm edm**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Access to EDM monitoring and configuration data is granted by default if XSM is enabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

## Usage Guidelines

This command exists to allow you to disable EDM using the **no xsm edm** form of the command. EDM is enabled by default when XSM is enabled.

EDM provides the following generic information to the VPN Device Manager (VDM):

- Relevant interfaces
- IP routing
- Access-list details
- Basic device health

Note that disabling EDM prevents XSM clients (such as VDM) from working properly and also disables the **xsm history edm** command. There is minimal performance impact associated with leaving EDM enabled.

---

**Examples**

In the following example, access to EDM data is disabled:

```
Router(config)# xsm  
Router(config)# no xsm edm
```

---

**Related Commands**

Command	Description
<b>xsm</b>	Enables XSM client access to the router.
<b>xsm dwdm</b>	Grants access to switch operations.
<b>xsm history edm</b>	Enables statistics collection for the EDM on the XSM server.
<b>xsm vdm</b>	Grants access to VPN-specific monitoring and configuration data.

# xsm history edm

To enable statistics collection for the Embedded Device Manager (EDM) on the XML Subscription Manager (XSM) server, use the **xsm history edm** command in global configuration mode. To disable statistics collection for the EDM on the XSM server, use the **no** form of this command.

**xsm history edm**

**no xsm history edm**

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

**Command Default** EDM statistics collection is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.1(6)E	This command was introduced.
	12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
	12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

**Usage Guidelines** Use this command to save up to five days of data. Historical information on items such as RAM and CPU utilization is gathered and made available, thus enabling XSM clients (such as VPN Device Manager [VDM]) to display charts and data. Use of this command consumes resources on the device. Disabling this command clears all your historical data, as the XSM server does not save this data between reloads.

**Examples** In the following example, statistics collection for the EDM is enabled on the XSM server:

```
Router(config)# xsm
Router(config)# xsm history edm
```

Related Commands	Command	Description
	xsm	Enables XSM client access to the router.

<b>Command</b>	<b>Description</b>
<b>xsm edm</b>	Grants access to EDM monitoring and configuration data.
<b>xsm history vdm</b>	Enables specific VPN statistics collection on the XSM server.

# xsm history vdm

To enable specific VPN statistics collection on the XML Subscription Manager (XSM) server, use the **xsm history vdm** command in global configuration mode. To disable collection of specific selected VPN statistics on the XSM server, use the **no** form of this command.

**xsm history vdm**

**no xsm history vdm**

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

**Command Default** VPN statistics collecting is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.1(6)E	This command was introduced.
	12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
	12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

**Usage Guidelines** With this command enabled, you can save up to five days of data. Historical information on items such as the number of active IKE tunnels, IPsec tunnels, total crypto throughput, and total throughput is gathered and made available, thus enabling XSM clients (such as VPN Device Manager [VDM]) to display charts and data. Use of this command consumes resources on the device. Disabling this command clears all your historical data. The XSM server does not save history data across reloads.

**Examples** The following example shows how to enable specific VPN statistics collection on the XSM server:

```
Router(config)# xsm
Router(config)# xsm history vdm
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>xsm</b>	Enables XSM client access to the router.
<b>xsm history edm</b>	Enables statistics collection for the EDM on the XSM server.
<b>xsm vdm</b>	Grants access to VPN-specific monitoring and configuration data.

# xsm privilege configuration level

To enable the XML Subscription Manager (XSM) configuration privilege level required to subscribe to XML Request Descriptors (XRDs), use the **xsm privilege configuration level** command in global configuration mode. To remove a previously configured XSM configuration privilege level, use the **no** form of this command.

**xsm privilege configuration level** *number*

**no xsm privilege configuration level** *number*

<b>Syntax Description</b>	<i>number</i>	Integer in the range from 1 to 15 that identifies the privilege level. The default is 15.
---------------------------	---------------	---

<b>Command Default</b>	The default level is 15.
------------------------	--------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(6)E	This command was introduced.
	12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
	12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

**Usage Guidelines** The privilege level for the **xsm privilege configuration level** command must be greater than or equal to the privilege level for the **xsm privilege monitor level** command. For example, if the **xsm privilege configuration 7** command is enabled, you need a minimum privilege level of 7 to subscribe to configuration XRDs. The higher the number the higher the privilege level. Trying to set a conflicting range of privilege settings will force the Cisco device to display the following message:

```
Attempt to set monitor privilege greater than configuration. Privilege denied.
```

You can check the XSM privilege level settings by using the **show xsm status** command. Use the **show xsm xrd-list** command to check which privilege level is required for each XRD.



## Note

The initial login set by your system administrator determines whether you have the necessary IOS privilege level for actually configuring the Cisco router. Ask your system administrator for more information about privilege levels.

**Examples**

The following example shows how to set a configuration privilege level of 15, and a monitor privilege level of 11 for subscription to XRDs. Users with a privilege level below 11 are denied access.

```
Router(config)# xsm privilege configuration level 15  
Router(config)# xsm privilege monitor level 11
```

**Related Commands**

Command	Description
privilege	Configures IOS privilege parameters.
xsm privilege monitor level	Enables monitor privilege level to subscribe to XRDs.

# xsm privilege monitor level

To enable the XML Subscription Manager (XSM) monitoring privilege level required to subscribe to XML Request Descriptors (XRDs), use the **xsm privilege monitor level** command in global configuration mode. To remove a previously configured XSM monitoring privilege level, use the **no** form of this command.

**xsm privilege monitor level** *number*

**no xsm privilege monitor level** *number*

<b>Syntax Description</b>	<i>number</i>	Integer in the range from 1 to 15 that identifies the privilege level. The default is 15.
---------------------------	---------------	---

<b>Command History</b>	The default is level 1.
------------------------	-------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(6)E	This command was introduced.
	12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
	12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

<b>Usage Guidelines</b>	The privilege level for the <b>xsm privilege monitor level</b> command must be less than or equal to the privilege level for the <b>xsm privilege configuration level</b> command. For example, if the <b>xsm privilege monitor 7</b> command is enabled, you need a minimum privilege level of 7 to subscribe to monitor XRDs. The higher the number the higher the privilege level. Trying to set a conflicting range of privilege settings will force the Cisco device to display the following message:
-------------------------	---

```
Attempt to set monitor privilege greater than configuration. Privilege denied.
```

You can check the XSM privilege level settings by using the **show xsm status** command. Use the **show xsm xrd-list** command to check which privilege level is required for each XRD.



## Note

The initial login set by your system administrator determines whether you have the necessary IOS privilege level for actually configuring the Cisco router. Ask your system administrator for more information about privilege levels.

---

**Examples**

The following example shows how to set a configuration privilege level of 15 and a monitor privilege level of 11 for subscription to XRDs. Users with a privilege level below 11 are denied access.

```
Router(config)# xsm privilege configuration level 15
Router(config)# xsm privilege monitor level 11
```

---

**Related Commands**

Command	Description
<b>privilege</b>	Configures IOS privilege parameters.
<b>xsm privilege configuration level</b>	Enables configuration privilege level to subscribe to XRDs.

# xsm vdm

To grant access to VPN-specific monitoring and configuration data for the VPN Device Manager (VDM), use the **xsm vdm** command in global configuration mode. To cancel access to VPN-specific monitoring and configuration data for VDM, use the **no** form of this command.

**xsm vdm**

**no xsm vdm**

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

**Command Default** Enabled (Access to VPN-specific monitoring and configuration data for the VDM is granted when XSM is enabled.)

**Command Modes** Global configuration

Command History	Release	Modification
	12.1(6)E	This command was introduced.
	12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
	12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

**Usage Guidelines** This command enables access to the following VPN-specific information:

- IPsec
- IKE
- Tunneling
- Encryption
- Keys and certificates

If XSM is enabled, this command is enabled by default. Access to VPN-specific monitoring and configuration data within XSM can be disabled by using the **no** form of the command. However, disabling this command will prevent VDM from working properly and will also disable the **xsm history vdm** command. Leaving this command enabled has minimal performance impact.

**Examples** In the following example, access to VPN-specific monitoring and configuration data is disabled:

```
Router(config)# xsm
Router(config)# no xsm vdm
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>xsm</b>	Enables XSM client access to the router.
<b>xsm dvd</b>	Grants access to switch operations.
<b>xsm edm</b>	Grants access to EDM monitoring and configuration data.
<b>xsm history vdm</b>	Enables specific VPN statistics collection on the XSM server.

