Network Management Commands

event manager applet

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

event manager applet *applet-name* [**authorization bypass**] [**class** *class-options*] [**trap**]
no event manager applet *applet-name* [**authorization bypass**] [**class** *class-options*] [**trap**]

Syntax Description	*applet-name*	Name of the applet file.
	authorization	(Optional) Specifies AAA authorization type for applet.
	bypass	(Optional) Specifies EEM AAA authorization type bypass.
	class	(Optional) Specifies the EEM policy class.
	class-options	(Optional) The EEM policy class. You can specify either one of the following: • *class-letter*-- Letter from A to Z that identifies each policy class. You can specify any one *class-letter*. • **default** --Specifies the policies registered with the default class.
	trap	(Optional) Generates a Simple Network Management Protocol (SNMP) trap when the policy is triggered.

Command Default No EEM applets are registered.

Command Modes

Global configuration (config)

Command History

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

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

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

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

Note Do not attempt making any partial modification. EEM does not support partial changes to already registered policies. EEM policy has to be always unregistered before registering again with changes.

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

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

The EEM policies will be assigned a class when **class** *class-letter* is specified when they are registered. EEM policies registered without a class will be assigned to the **default** class. Threads that have **default** as the class will service the default class when the thread is available for work. Threads that are assigned specific class letters will service any policy with a matching class letter when the thread is available for work.

If there is no EEM execution thread available to run the policy in the specified class and a scheduler rule for the class is configured, the policy will wait until a thread of that class is available for execution. Synchronous policies that are triggered from the same input event should be scheduled in the same execution thread. Policies will be queued in a separate queue for each class using the queue_priority as the queuing order.

When a policy is triggered and if AAA is configured it will contact the AAA server for authorization. Using the **authorization bypass** keyword combination, you can skip to contact the AAA server and run the policy immediately. EEM stores AAA bypassed policy names in a list. This list is checked when policies are triggered. If a match is found, AAA authorization is bypassed.

To avoid authorization for commands configured through the EEM policy, EEM will use named method lists, which AAA provides. These named method lists can be configured to have no command authorization.

The following is a sample AAA configuration.

This configuration assumes a TACACS+ server at 192.168.10.1 port 10000. If the TACACS+ server is not enabled, configuration commands are permitted on the console; however, EEM policy and applet CLI interactions will fail.

```
enable password lab
aaa new-model
tacacs-server host 128.107.164.152 port 10000
tacacs-server key cisco
aaa authentication login consoleline none
aaa authorization exec consoleline none
aaa authorization commands 1 consoleline none
aaa authorization commands 15 consoleline none
line con 0
 exec-timeout 0 0
 login authentication consoleline
aaa authentication login default group tacacs+ enable
aaa authorization exec default group tacacs+
aaa authorization commands 1 default group tacacs+
aaa authorization commands 15 default group tacacs+
```

The **authorization**, **class** and **trap** keywords can be used in any combination.

Examples

The following example shows an EEM applet called IPSLAping1 being registered to run when there is an exact match on the value of a specified SNMP object ID that represents a successful IP SLA

ICMP echo operation (this is equivalent to a **ping** command). Four actions are triggered when the echo operation fails, and event monitoring is disabled until after the second failure. A message that the ICMP echo operation to a server failed is sent to syslog, an SNMP trap is generated, EEM publishes an application-specific event, and a counter called IPSLA1F is incremented by a value of one.

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

The following example shows how to register an applet with the name one and class A and enter applet configuration mode where the timer event detector is set to trigger an event every 10 seconds. When the event is triggered, the **action syslog** command writes the message "hello world" to syslog.

```
Router(config)# event manager applet one class A
Router(config-applet)# event timer watchdog time 10
Router(config-applet)# action syslog syslog msg "hello world"
Router(config-applet)# exit
```

The following example shows how to bypass the AAA authorization when registering an applet with the name one and class A.

```
Router(config)# event manager applet one class A authorization bypass
Router(config-applet)#
```

Related Commands

Command	Description
show event manager policy registered	Displays registered EEM policies.

ip wccp

To enable the web cache service, and specify the service number that corresponds to a dynamic service that is defined by the application engine, use the **ip wccp** global configuration command on the device. Use the **no** form of this command to disable the service.

ip wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]
no ip wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]

Syntax Description		
	web-cache	Specifies the web-cache service (WCCP Version 1 and Version 2).
	service-number	Dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254. The maximum number of services is 256, which includes the web-cache service specified with the **web-cache** keyword.
	group-address *groupaddress*	(Optional) Specifies the multicast group address used by the device and the application engines to participate in the service group.
	group-list *access-list*	(Optional) If a multicast group address is not used, specifies a list of valid IP addresses that correspond to the application engines that are participating in the service group.
	redirect-list *access-list*	(Optional) Specifies the redirect service for specific hosts or specific packets from hosts.
	password *encryption-number password*	(Optional) Specifies an encryption number. The range is 0 to 7. Use 0 for not encrypted, and use 7 for proprietary. Also, specifies a password name up to seven characters in length. The device combines the password with the MD5 authentication value to create security for the connection between the device and the application engine. By default, no password is configured, and no authentication is performed.

Command Default

WCCP services are not enabled on the device.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when Cisco Express Forwarding switching is enabled. To work around this situation, configure WCCP transparent caching in the outgoing direction, enable Cisco Express Forwarding switching on the content engine interface, and specify the **ip wccp web-cache redirect out** command. Configure WCCP in the incoming direction on the inside interface by

specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This configuration prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group. The specified redirect list will deny packets with a NAT (source) IP address and prevent redirection.

This command instructs a device to enable or disable support for the specified service number or the web-cache service name. A service number can be from 0 to 254. Once the service number or name is enabled, the router can participate in the establishment of a service group.

When the **no ip wccp** command is entered, the device terminates participation in the service group, deallocates space if none of the interfaces still have the service configured, and terminates the WCCP task if no other services are configured.

The keywords following the **web-cache** keyword and the *service-number* argument are optional and may be specified in any order, but only may be specified once.

Example

The following example configures a web cache, the interface connected to the application engine or the server, and the interface connected to the client:

```
Device(config)# ip wccp web-cache
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no switchport
Device(config-if)# ip address 172.20.10.30 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport
Device(config-if)#
*Dec  6 13:11:29.507: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to down

Device(config-if)# ip address 175.20.20.10 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# ip wccp web-cache group-listen
Device(config-if)# exit
```

map platform-type

To set the parameter map attribute filter criteria to platform type, use the **map platform-type** command in parameter-map filter mode. To remove this criteria, use the **no** form of this command.

map-number **map platform-type** {{**eq** | **not-eq** | **regex**} *platform-type*}
no *map-number* **map platform-type** {{**eq** | **not-eq** | **regex**} *platform-type*}

Syntax Description		
	map-number	Parameter map number.
	eq	Specifies that the filter type name is equal to the platform type name.
	not-eq	Specifies that the filter type name is not equal to the platform type name.
	regex	Specifies that the filter type name is a regular expression.
	platform-type	Platform type for the parameter map attribute filter criteria.

Command Default   No default behavior or values.

Command Modes   Parameter-map filter (config-parameter-map-filter)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Examples   The following example shows how to set the parameter map attribute filter criteria to platform type:

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para
Device(config-parameter-map-filter)# 10 map platform-type eq C9xxx
```

Related Commands	Command	Description
	parameter-map type subscriber attribute-to-service	Configures a subscriber parameter map and enters parameter-map filter configuration mode.

match platform-type

To evaluate control classes based on the platform type, use the **match platform-type** command in control class-map filter mode. To remove this condition, use the **no** form of this command.

match platform-type *platform-name*
no match platform-type *platform-name*

Syntax Description

platform-name	Name of the platform.

Command Default   No default behavior or values.

Command Modes   Control class-map filter (config-filter-control-classmap)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Examples   The following example shows how to set a class map filter to match a platform type:

```
Device> enable
Device# configure terminal
Device(config)# class-map type control subscriber match-all DOT1X_NO_AGENT
Device(config-filter-control-classmap)# match platform-type C9xxx
```

Related Commands

Command	Description
class-map type control subscriber	Creates a control class and enters control class-map filter mode.

monitor capture (interface/control plane)

To configure monitor capture points specifying an attachment point and the packet flow direction or add more attachment points to a capture point, use the **monitor capture** command in privileged EXEC mode. To disable the monitor capture with the specified attachment point and the packet flow direction or disable one of multiple attachment points on a capture point, use the **no** form of this command.

monitor capture {*capture-name*} {**interface** *interface-type* *interface-id* | **control-plane**} {**in** | **out** | **both**}
no monitor capture {*capture-name*} {**interface** *interface-type* *interface-id* | **control-plane**} {**in** | **out** | **both**}

Syntax Description

capture-name	The name of the capture to be defined.
interface *interface-type* *interface-id*	Specifies an interface with *interface-type* and *interface-id* as an attachment point. The arguments have these meanings: • **GigabitEthernet** *interface-id*—A Gigabit Ethernet IEEE 802.3z interface. • **vlan** *vlan-id*—A VLAN. The range for *vlan-id* is 1 to 4095.
control-plane	Specifies the control plane as an attachment point.
in | **out** | **both**	Specifies the traffic direction to be captured.

Command Default A Wireshark capture is not configured.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines Once an attachment point has been associated with a capture point using this command, the only way to change its direction is to remove the attachment point using the **no** form of the command and reattach the attachment point with the new direction. An attachment point's direction cannot be overridden.

If an attachment point is removed from a capture point and only one attachment point is associated with it, the capture point is effectively deleted.

Multiple attachment points can be associated with a capture point by re-running this command with another attachment point. An example is provided below.

Packets captured in the output direction of an interface might not reflect the changes made by switch rewrite (includes TTL, VLAN tag, CoS, checksum, MAC addresses, DSCP, precedent, UP, etc.).

No specific order applies when defining a capture point; you can define capture point parameters in any order. The Wireshark CLI allows as many parameters as possible on a single line. This limits the number of commands required to define a capture point.

Neither VRFs, management ports, nor private VLANs can be used as attachment points.

Wireshark cannot capture packets on a destination SPAN port.

When a VLAN is used as a Wireshark attachment point, packets are captured in the input direction only.

Examples

To define a capture point using a physical interface as an attachment point:

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
```

Note The second command defines the core filter for the capture point. This is required for a functioning capture point.

To define a capture point with multiple attachment points:

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap control-plane in
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap control-plane in
```

To remove an attachment point from a capture point defined with multiple attachment points:

```
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap control-plane in
Device# no monitor capture mycap control-plane
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
```

monitor capture buffer

To configure the buffer for monitor capture (WireShark), use the **monitor capture buffer** command in privileged EXEC mode. To disable the monitor capture buffer or change the buffer back to a default linear buffer from a circular buffer, use the **no** form of this command.

monitor capture {*capture-name*} **buffer** {**circular** [**size** *buffer-size*] | **size** *buffer-size*}
no monitor capture {*capture-name*} **buffer** [**circular**]

Syntax Description		
capture-name	The name of the capture whose buffer is to be configured.
circular	Specifies that the buffer is of a circular type. The circular type of buffer continues to capture data, even after the buffer is consumed, by overwriting the data captured previously.
size *buffer-size*	(Optional) Specifies the size of the buffer. The range is from 1 MB to 100 MB.

Command Default A linear buffer is configured.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines When you first configure a WireShark capture, a circular buffer of a small size is suggested.

Example

To configure a circular buffer with a size of 1 MB:

```
Device# monitor capture mycap buffer circular size 1
```

monitor capture export

To export a monitor capture (WireShark) to a file, use the **monitor capture export** command in privileged EXEC mode.

monitor capture {*capture-name*} **export** *file-location* **:** *file-name*

Syntax Description	*capture-name*	The name of the capture to be exported.
	file-location : *file-name*	(Optional) Specifies the location and file name of the capture storage file. Acceptable values for *file-location* :
		• flash—On-board flash storage
		• — USB drive

Command Default	The captured packets are not stored.

Command Modes	Privileged EXEC

Command History	**Release**	**Modification**
		This command was introduced.

Usage Guidelines

Use the **monitor capture export** command only when the storage destination is a capture buffer. The file may be stored either remotely or locally. Use this command either during capture or after the packet capture has stopped. The packet capture is stopped when one or more end conditions have been met or you entered the **monitor capture stop** command.

When WireShark is used on switches in a stack, packet captures can be stored only on the devices specified for *file-location* above that are connected to the active switch. Example: flash1 is connected to the active switch. flash2 is connected to the secondary switch. Only flash1 can be used to store packet captures.

✎

Note   Attempts to store packet captures on unsupported devices or devices not connected to the active switch will probably result in errors.

Example

To export the capture buffer contents to mycap.pcap on a flash drive:

monitor capture limit

To configure capture limits, use the **monitor capture limit** command in privileged EXEC mode. To remove the capture limits, use the **no** form of this command.

monitor capture {*capture-name*} **limit** {[**duration** *seconds*] [**packet-length** *size*] [**packets** *num*]}
no monitor capture {*capture-name*} **limit** [**duration**] [**packet-length**] [**packets**]

Syntax Description		
	capture-name	The name of the capture to be assigned capture limits.
	duration *seconds*	(Optional) Specifies the duration of the capture, in seconds. The range is from 1 to 1000000.
	packet-length *size*	(Optional) Specifies the packet length, in bytes. If the actual packet is longer than the specified length, only the first set of bytes whose number is denoted by the bytes argument is stored.
	packets *num*	(Optional) Specifies the number of packets to be processed for capture.

Command Default Capture limits are not configured.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

To configure a session limit of 60 seconds and a packet segment length of 400 bytes:

```
Device# monitor capture mycap limit duration 60 packet-len 400
```

monitor capture start

To start the capture of packet data at a traffic trace point into a buffer, use the **monitor capture start** command in privileged EXEC mode.

monitor capture {*capture-name*} **start**

Syntax Description	*capture-name*	The name of the capture to be started.

Command Default   The buffer content is not cleared.

Command Modes   Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines   Use the **monitor capture clear** command to enable the packet data capture after the capture point is defined. To stop the capture of packet data, use the **monitor capture stop** command.

Ensure that system resources such as CPU and memory are available before starting a capture.

Example

To start capturing buffer contents:

```
Device#  monitor capture mycap start
```

monitor capture stop

To stop the capture of packet data at a traffic trace point, use the **monitor capture stop** command in privileged EXEC mode.

monitor capture {*capture-name*} **stop**

Syntax Description

capture-name	The name of the capture to be stopped.

Command Default   The packet data capture is ongoing.

Command Modes   Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines   Use the **monitor capture stop** command to stop the capture of packet data that you started using the **monitor capture start** command. You can configure two types of capture buffers: linear and circular. When the linear buffer is full, data capture stops automatically. When the circular buffer is full, data capture starts from the beginning and the data is overwritten.

Example

To stop capturing buffer contents:

```
Device#  monitor capture mycap stop
```

monitor session destination

To start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) destination session, to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance), and to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, use the **monitor session destination** global configuration command. To remove the SPAN or RSPAN session or to remove destination interfaces from the SPAN or RSPAN session, use the **no** form of this command.

monitor session *session-number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**replicate** | **dot1q**}] {**ingress** [**dot1q** | **untagged**] } | {**remote**} **vlan** *vlan-id*
no monitor session *session-number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**replicate** | **dot1q**}] {**ingress** [**dot1q** | **untagged**] } | {**remote**} **vlan** *vlan-id*

Syntax Description		
session-number		
interface *interface-id*		Specifies the destination or source interfa physical ports (including type, stack mem channel is also a valid interface type, and
,		(Optional) Specifies a series of interfaces from a previous range. Enter a space befo
-		(Optional) Specifies a range of interfaces
encapsulation replicate		(Optional) Specifies that the destination int If not selected, the default is to send pack
		These keywords are valid only for local S original VLAN ID; therefore, packets are ignored with the **no** form of the command
encapsulation dot1q		(Optional) Specifies that the destination in IEEE 802.1Q encapsulation.
		These keywords are valid only for local S original VLAN ID; therefore, packets are ignored with the **no** form of the command
ingress		Enables ingress traffic forwarding.
dot1q		(Optional) Accepts incoming packets with the default VLAN.
untagged		(Optional) Accepts incoming packets with default VLAN.
isl		Specifies ingress forwarding using ISL en
remote		Specifies the remote VLAN for an RSPAN 1006 to 4094.
		The RSPAN VLAN cannot be VLAN 1 (t for Token Ring and FDDI VLANs).

vlan *vlan-id*	Sets the default VLAN for ingress traffic whe

Command Default	No monitor sessions are configured.
	If **encapsulation replicate** is not specified on a local SPAN destination port, packets are sent in native form with no encapsulation tag.
	Ingress forwarding is disabled on destination ports.
	You can specify **all**, **local**, **range** *session-range*, or **remote** with the **no monitor session** command to clear all SPAN and RSPAN, all local SPAN, a range, or all RSPAN sessions.

Command Modes	Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines A SPAN or RSPAN destination must be a physical port.

You can have a maximum of 64 destination ports on a switch or a switch stack.

Each session can include multiple ingress or egress source ports or VLANs, but you cannot combine source ports and source VLANs in a single session. Each session can include multiple destination ports.

When you use VLAN-based SPAN (VSPAN) to analyze network traffic in a VLAN or set of VLANs, all active ports in the source VLANs become source ports for the SPAN or RSPAN session. Trunk ports are included as source ports for VSPAN, and only packets with the monitored VLAN ID are sent to the destination port.

You can monitor traffic on a single port or VLAN or on a series or range of ports or VLANs. You select a series or range of interfaces or VLANs by using the [**,** | **-**] options.

If you specify a series of VLANs or interfaces, you must enter a space before and after the comma. If you specify a range of VLANs or interfaces, you must enter a space before and after the hyphen (**-**).

EtherChannel ports can be configured as SPAN or RSPAN destination ports. A physical port that is a member of an EtherChannel group can be used as a destination port, but it cannot participate in the EtherChannel group while it is as a SPAN destination.

A port used as a destination port cannot be a SPAN or RSPAN source, nor can a port be a destination port for more than one session at a time.

You can enable IEEE 802.1x authentication on a port that is a SPAN or RSPAN destination port; however, IEEE 802.1x authentication is disabled until the port is removed as a SPAN destination. If IEEE 802.1x authentication is not available on the port, the switch returns an error message. You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.

If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.

Destination ports can be configured to function in these ways:

- When you enter **monitor session** *session_number* **destination interface** *interface-id* with no other keywords, egress encapsulation is untagged, and ingress forwarding is not enabled.

- When you enter **monitor session** *session_number* **destination interface** *interface-id* **ingress**, egress encapsulation is untagged; ingress encapsulation depends on the keywords that follow—**dot1q** or **untagged**.

- When you enter **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate** with no other keywords, egress encapsulation replicates the source interface encapsulation; ingress forwarding is not enabled. (This applies to local SPAN only; RSPAN does not support encapsulation replication.)

- When you enter **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate ingress**, egress encapsulation replicates the source interface encapsulation; ingress encapsulation depends on the keywords that follow—**dot1q** or **untagged**. (This applies to local SPAN only; RSPAN does not support encapsulation replication.)

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

Examples

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2:

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

This example shows how to delete a destination port from an existing local SPAN session:

```
Device(config)# no monitor session 2 destination interface gigabitethernet1/0/2
```

This example shows how to configure RSPAN source session 1 to monitor a source interface and to configure the destination RSPAN VLAN 900:

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
Device(config)# monitor session 1 destination remote vlan 900
Device(config)# end
```

This example shows how to configure an RSPAN destination session 10 in the switch receiving the monitored traffic:

```
Device(config)# monitor session 10 source remote vlan 900
Device(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports IEEE 802.1Q encapsulation. Egress traffic replicates the source; ingress traffic uses IEEE 802.1Q encapsulation.

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
 dot1q ingress dot1q vlan 5
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that does not support encapsulation. Egress traffic and ingress traffic are untagged.

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress untagged
 vlan 5
```

monitor session filter

To start a new flow-based SPAN (FSPAN) session or flow-based RSPAN (FRSPAN) source or destination session, or to limit (filter) SPAN source traffic to specific VLANs, use the **monitor session filter** global configuration command. To remove filters from the SPAN or RSPAN session, use the **no** form of this command.

monitor session *session-number* **filter** { **vlan** *vlan-id* [**,** | **-**] }
no monitor session *session-number* **filter** { **vlan** *vlan-id* [**,** | **-**] }

Syntax Description	*session-number*	
	vlan *vlan-id*	Specifies a list of VLANs as filters on trunk source ports t VLANs. The *vlan-id* range is 1 to 4094.
	,	(Optional) Specifies a series of VLANs, or separates a ra Enter a space before and after the comma.
	-	(Optional) Specifies a range of VLANs. Enter a space be

Command Default No monitor sessions are configured.

Command Modes Global configuration

Command History	**Release**	**Modification**
	Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines You can monitor traffic on a single VLAN or on a series or range of ports or VLANs. You select a series or range of VLANs by using the [**,** | **-**] options.

If you specify a series of VLANs, you must enter a space before and after the comma. If you specify a range of VLANs, you must enter a space before and after the hyphen (**-**).

VLAN filtering refers to analyzing network traffic on a selected set of VLANs on trunk source ports. By default, all VLANs are monitored on trunk source ports. You can use the **monitor session** *session_number* **filter vlan** *vlan-id* command to limit SPAN traffic on trunk source ports to only the specified VLANs.

VLAN monitoring and VLAN filtering are mutually exclusive. If a VLAN is a source, VLAN filtering cannot be enabled. If VLAN filtering is configured, a VLAN cannot become a source.

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

Examples

This example shows how to limit SPAN traffic in an existing session only to specific VLANs:

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2 and to filter IPv4 traffic using access list number 122 in an FSPAN session:

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
Device(config)# monitor session 1 filter ip access-group 122
```

monitor session source

To start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) source session, or to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, use the **monitor session source** global configuration command. To remove the SPAN or RSPAN session or to remove source interfaces from the SPAN or RSPAN session, use the **no** form of this command.

monitor session *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [**,** | **-**] [**both** | **rx** | **tx**]}
no monitor session *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [**,** | **-**] [**both** | **rx** | **tx**]}

Syntax Description		
	session_number	
	interface *interface-id*	Specifies the source interface for a SPAN or RSPAN session. Valid interfaces are physical ports (including type, stack member, module, and port number). For source interface, port channel is also a valid interface type, and the valid range is 1 to 48.
	,	(Optional) Specifies a series of interfaces or VLANs, or separates a range of interfaces or VLANs from a previous range. Enter a space before and after the comma.
	-	(Optional) Specifies a range of interfaces or VLANs. Enter a space before and after the hyphen.
	both | **rx** | **tx**	(Optional) Specifies the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic.
	remote	(Optional) Specifies the remote VLAN for an RSPAN source or destination session. The range is 2 to 1001 and 1006 to 4094.
		The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).
	vlan *vlan-id*	When used with only the **ingress** keyword, sets default VLAN for ingress traffic.

Command Default

No monitor sessions are configured.

On a source interface, the default is to monitor both received and transmitted traffic.

On a trunk interface used as a source port, all VLANs are monitored.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines Traffic that enters or leaves source ports or source VLANs can be monitored by using SPAN or RSPAN. Traffic routed to source ports or source VLANs cannot be monitored.

A source can be a physical port, a port channel, or a VLAN.

Each session can include multiple ingress or egress source ports or VLANs, but you cannot combine source ports and source VLANs in a single session. Each session can include multiple destination ports.

When you use VLAN-based SPAN (VSPAN) to analyze network traffic in a VLAN or set of VLANs, all active ports in the source VLANs become source ports for the SPAN or RSPAN session. Trunk ports are included as source ports for VSPAN, and only packets with the monitored VLAN ID are sent to the destination port.

You can monitor traffic on a single port or VLAN or on a series or range of ports or VLANs. You select a series or range of interfaces or VLANs by using the [**,** | **-**] options.

If you specify a series of VLANs or interfaces, you must enter a space before and after the comma. If you specify a range of VLANs or interfaces, you must enter a space before and after the hyphen (**-**).

You can monitor individual ports while they participate in an EtherChannel, or you can monitor the entire EtherChannel bundle by specifying the **port-channel** number as the RSPAN source interface.

A port used as a destination port cannot be a SPAN or RSPAN source, nor can a port be a destination port for more than one session at a time.

You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

Examples

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2:

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

This example shows how to configure RSPAN source session 1 to monitor multiple source interfaces and to configure the destination RSPAN VLAN 900.

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

show class-map type control subscriber

To display the class map statistics for the configured control policies, use the **show class-map type control subscriber** command in privileged EXEC mode.

show class-map type control subscriber {all | name *control-class-name*}

Syntax Description		
all		Displays class map statistics for all control policies.
name *control-class-name*		Displays class map statistics for the specified control policy.

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Examples

The following is a sample output of the **show class-map type control subscriber name** *control-class-name* command:

```
Device# show class-map type control subscriber name platform

Class-map               Action               Exec  Hit  Miss  Comp
---------               ------               ----  ---  ----  ----
match-all platform      match platform-type C9xxx  0    0    0    0
Key:
  "Exec" - The number of times this line was executed
  "Hit"  - The number of times this line evaluated to TRUE
  "Miss" - The number of times this line evaluated to FALSE
  "Comp" - The number of times this line completed the execution of its
       condition without a need to continue on to the end
```

show ip sla statistics

To display current or aggregated operational status and statistics of all Cisco IOS IP Service Level Agreement (SLA) operations or a specified operation, use the **show ip sla statistics** command in user EXEC or privileged EXEC mode.

show ip sla statistics [*operation-number* [**details**] | **aggregated** [*operation-number* | **details**] | **details**]

Syntax Description

operation-number	(Optional) Number of the operation for which operational status and statistics are displayed. Accepted values are from 1 to 2147483647.
details	(Optional) Specifies detailed output.
aggregated	(Optional) Specifies the IP SLA aggregated statistics.

Command Default   Displays output for all running IP SLA operations.

Command Modes   User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines   Use the **show ip sla statistics** to display the current state of IP SLA operations, including how much life the operation has left, whether the operation is active, and the completion time. The output also includes the monitoring data returned for the last (most recently completed) operation. This generated operation ID is displayed when you use the **show ip sla** configuration command for the base multicast operation, and as part of the summary statistics for the entire operation.

Enter the **show** command for a specific operation ID to display details for that one responder.

Examples

The following is sample output from the **show ip sla statistics** command:

```
Device# show ip sla statistics

Current Operational State
Entry Number: 3
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
Operational State of Entry: active
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200  OK
```

```
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707
```

show monitor

To display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions, use the **show monitor** command in EXEC mode.

show monitor [**session** {*session_number* | **all** | **local** | **range** *list* | **remote**} [**detail**]]

Syntax Description	

session	(Optional) Displays information about specified SPAN sessions.
session_number	
all	(Optional) Displays all SPAN sessions.
local	(Optional) Displays only local SPAN sessions.
range *list*	(Optional) Displays a range of SPAN sessions, where *list* is the range of valid sessions. The range is either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges.
	Note This keyword is available only in privileged EXEC mode.
remote	(Optional) Displays only remote SPAN sessions.
detail	(Optional) Displays detailed information about the specified sessions.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The output is the same for the **show monitor** command and the **show monitor session all** command.

Examples

This is an example of output for the **show monitor** user EXEC command:

```
Device# show monitor
Session 1
---------
Type : Local Session
Source Ports :
```

```
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
Session 2
---------
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

This is an example of output for the **show monitor** user EXEC command for local SPAN source session 1:

```
Device# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

This is an example of output for the **show monitor session all** user EXEC command when ingress traffic forwarding is enabled:

```
Device# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
---------
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/012
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

show monitor capture

To display monitor capture (WireShark) content, use the **show monitor capture** command in privileged EXEC mode.

show monitor capture [*capture-name* [**buffer**] | **file** *file-location* **:** *file-name*] [**brief** | **detailed** | **display-filter** *display-filter-string*]

Syntax Description

capture-name	(Optional) Specifies the name of the capture to be displayed.
buffer	(Optional) Specifies that a buffer associated with the named capture is to be displayed.
file *file-location* : *file-name*	(Optional) Specifies the file location and name of the capture storage file to be displayed.
brief	(Optional) Specifies the display content in brief.
detailed	(Optional) Specifies detailed display content.
display-filter *display-filter-string*	Filters the display content according to the *display-filter-string*.

Command Default   Displays all capture content.

Command Modes   Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

The following is sample output from the **show monitor capture** command:

```
Device# show monitor capture mycap

Status Information for Capture mycap
 Target Type:
 Interface: CAPWAP,
   Ingress:
0
   Egress:
0
  Status : Active
 Filter Details:
   Capture all packets
 Buffer Details:
  Buffer Type: LINEAR (default)
 File Details:
  Associated file name: flash:mycap.pcap
  Size of buffer(in MB): 1
 Limit Details:
  Number of Packets to capture: 0 (no limit)
```

```
Packet Capture duration: 0 (no limit)
Packet Size to capture: 0 (no limit)
Packets per second: 0 (no limit)
Packet sampling rate: 0 (no sampling)
```

show parameter-map type subscriber attribute-to-service

To display parameter map statistics, use the **show parameter-map type subscriber attribute-to-service** command in privileged EXEC mode.

show parameter-map type subscriber attribute-to-service {all | name *parameter-map-name***}**

Syntax Description

all	Displays statistics for all parameter maps.
name *parameter-map-name*	Displays statistics for the specified parameter map.

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Examples   The following is a sample output of the **show parameter-map type subscriber attribute-to-service name** *parameter-map-name* command:

```
Device# show parameter-map type subscriber attribute-to-service name platform


Parameter-map name: platform
 Map: 10 platform-type regex "C9xxx"
  Action(s):
     10 interface-template critical
```

show platform software fed switch ip wccp

To display platform-dependent Web Cache Communication Protocol (WCCP) information, use the **show platform software fed switch ip wccp** privileged EXEC command.

```
show platform software fed switch{switch-number|active|standby}ip
wccp{cache-engines |interfaces |service-groups}
```

Syntax Description	**switch**{*switch_num*|**active**|**standby**}	The device for which you want to display information.
		• *switch_num*—Enter the switch ID. Displays information for the specified switch.
		• **active**—Displays information for the active switch.
		• **standby**—Displays information for the standby switch, if available.
	cache-engines	Displays WCCP cache engines.
	interfaces	Displays WCCP interfaces.
	service-groups	Displays WCCP service groups.

Command Modes   Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines   Use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

This command is available only if your device is running the IP Services feature set.

The following example displays WCCP interfaces:

```
Device# show platform software fed switch 1 ip wccp interfaces

WCCP Interface Info

====================

**** WCCP Interface: Port-channel13 iif_id: 000000000000007c (#SG:3),  VRF: 0 Ingress WCCP
 ****
port_handle:0x20000f9

List of Service Groups on this interface:
* Service group id:90 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP     l4_type: Dest ports     priority: 35
Promiscuous mode (no ports).
```

```
* Service group id:70 vrf_id:0 (ref count:24)
type: Dynamic     Open service     prot: PROT_TCP    l4_type: Dest ports     priority: 35
Promiscuous mode (no ports).


* Service group id:60 vrf_id:0 (ref count:24)
type: Dynamic     Open service     prot: PROT_TCP    l4_type: Dest ports     priority: 35
Promiscuous mode (no ports).



**** WCCP Interface: Port-channel14 iif_id: 000000000000007e (#SG:3),  VRF: 0 Ingress WCCP
 ****
port_handle:0x880000fa

List of Service Groups on this interface:
* Service group id:90 vrf_id:0 (ref count:24)
type: Dynamic     Open service     prot: PROT_TCP    l4_type: Dest ports     priority: 35
Promiscuous mode (no ports).


* Service group id:70 vrf_id:0 (ref count:24)
type: Dynamic     Open service     prot: PROT_TCP    l4_type: Dest ports     priority: 35
Promiscuous mode (no ports).
<output truncated>
```

show platform software swspan

To display switched port analyzer (SPAN) information, use the **show platform software swspan** command in privileged EXEC mode.

show platform software swspan {**switch**} {{{**F0** |**FP active**} **counters**}|**R0** |**RP active**} {**destination sess-id** *session-ID* |**source sess-id** *session-ID*}

Syntax Description		
	switch	Displays information about the switch.
	F0	Displays information about the Embedded Service Processor (ESP) slot 0.
	FP	Displays information about the ESP.
	active	Displays information about the active instance of the ESP or the Route Processor (RP).
	counters	Displays the SWSPAN message counters.
	R0	Displays information about the RP slot 0.
	RP	Displays information the RP.
	destination sess-id *session-ID*	Displays information about the specified destination session.
	source sess-id *session-ID*	Displays information about the specified source session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced in a release prior to Cisco IOS XE Denali 16.1.1.

Usage Guidelines

If the session number does not exist or if the SPAN session is a remote destination session, the command output will display the following message "% Error: No Information Available."

Examples

The following is sample output from the **show platform software swspan FP active source** command:

```
Switch# show platform software swspan FP active source sess-id 0

Showing SPAN source detail info

Session ID : 0
Intf Type : PORT
Port dpidx : 30
PD Sess ID : 1
Session Type : Local
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 579
```

```
AOM Object Status : Done
Parent AOM object Id : 118
Parent AOM object Status : Done

Session ID : 9
Intf Type : PORT
Port dpidx : 8
PD Sess ID : 0
Session Type : Local
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 578
AOM Object Status : Done
Parent AOM object Id : 70
Parent AOM object Status : Done
```

The following is sample output from the **show platform software swspan RP active destination** command:

```
Switch# show platform software swspan RP active destination

Showing SPAN destination table summary info

Sess-id IF-type IF-id Sess-type
------------------------------------
1 PORT 19 Remote
```

snmp ifmib ifindex persist

To globally enable ifIndex values to persist , which will remain constant across reboots, for use by the Simple Network Management Protocol (SNMP), use the **snmp ifmib ifindex persist** command in global configuration mode. To globally disable ifIndex persistence, use the **no** form of this command.

snmp ifmib ifindex persist
no snmp ifmib ifindex persist

Syntax Description	This command has no arguments or keywords.
Command Default	The ifIndex persistence on a device is disabled.
Command Modes	Global configuration (config)
Usage Guidelines	The **snmp ifmib ifindex persist** command does not override an interface-specific configuration. The interface-specific configuration of ifIndex persistence is configured with the **snmp ifindex persist** and **snmp ifindex clear** commands in interface configuration mode.

The **snmp ifmib ifindex persist** command enables ifIndex persistence for all interfaces on a routing device by using the ifDescr and ifIndex entries in the ifIndex table of interface MIB (IF-MIB).

ifIndex persistence means that the ifIndex values in the IF-MIB persist across reboots, allowing for the consistent identification of specific interfaces that use SNMP.

If ifIndex persistence was previously disabled for a specific interface by using the **no snmp ifindex persist** command, ifIndex persistence will remain disabled for that interface.

Examples

The following example shows how to enable ifIndex persistence for all interfaces:

```
Device(config)# snmp ifmib ifindex persist
```

Related Commands

Command	Description
snmp ifindex clear	Clears any previously configured **snmp ifIndex** commands issued in interface configuration mode for a specific interface.
snmp ifindex persist	Enables ifIndex values that persist across reboots (ifIndex persistence) in the IF-MIB.

snmp-server enable traps

To enable the device to send Simple Network Management Protocol (SNMP) notifications for various traps or inform requests to the network management system (NMS), use the **snmp-server enable traps** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps [**auth-framework** [**sec-violation**] | **bridge** | **call-home** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp**]
no snmp-server enable traps [**auth-framework** [**sec-violation**] | **bridge** | **call-home** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp**]

Syntax Description		
auth-framework		(Optional) Enables SNMP CISCO-AUTH-FRAMEWORK-MIB traps.
sec-violation		(Optional) Enables SNMP camSecurityViolationNotif notifications.
bridge		(Optional) Enables SNMP STP Bridge MIB traps.*
call-home		(Optional) Enables SNMP CISCO-CALLHOME-MIB traps.*
config		(Optional) Enables SNMP configuration traps.
config-copy		(Optional) Enables SNMP configuration copy traps.
config-ctid		(Optional) Enables SNMP configuration CTID traps.
copy-config		(Optional) Enables SNMP copy-configuration traps.
cpu		(Optional) Enables CPU notification traps.*
dot1x		(Optional) Enables SNMP dot1x traps.*
energywise		(Optional) Enables SNMP energywise traps.*
entity		(Optional) Enables SNMP entity traps.
envmon		(Optional) Enables SNMP environmental monitor traps.*
errdisable		(Optional) Enables SNMP errdisable notification traps.*
event-manager		(Optional) Enables SNMP Embedded Event Manager traps.
flash		(Optional) Enables SNMP FLASH notification traps.*

fru-ctrl	(Optional) Generates entity field-replaceable unit (FRU) control traps. In a device stack, this trap refers to the insertion or removal of a device in the stack.
license	(Optional) Enables license traps.*
mac-notification	(Optional) Enables SNMP MAC Notification traps.*
port-security	(Optional) Enables SNMP port security traps.*
power-ethernet	(Optional) Enables SNMP power Ethernet traps.*
rep	(Optional) Enables SNMP Resilient Ethernet Protocol traps.
snmp	(Optional) Enables SNMP traps.*
stackwise	(Optional) Enables SNMP stackwise traps.*
storm-control	(Optional) Enables SNMP storm-control trap parameters.*
stpx	(Optional) Enables SNMP STPX MIB traps.*
syslog	(Optional) Enables SNMP syslog traps.
transceiver	(Optional) Enables SNMP transceiver traps.*
tty	(Optional) Sends TCP connection traps. This is enabled by default.
vlan-membership	(Optional) Enables SNMP VLAN membership traps.
vlancreate	(Optional) Enables SNMP VLAN-created traps.
vlandelete	(Optional) Enables SNMP VLAN-deleted traps.
vstack	(Optional) Enables SNMP Smart Install traps.*
vtp	(Optional) Enables VLAN Trunking Protocol (VTP) traps.

Command Default

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The command options marked with an asterisk in the table above have subcommands. For more information on these subcommands, see the Related Commands section below.

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

When supported, use the **snmp-server enable traps** command to enable sending of traps or informs.

Note Though visible in the command-line help strings, the **fru-ctrl, insertion**, and **removal** keywords are not supported on the device. The **snmp-server enable informs** global configuration command is not supported. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** global configuration command combined with the **snmp-server host** *host-addr* **informs** global configuration command.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples This example shows how to enable more than one type of SNMP trap:

```
Device(config)# snmp-server enable traps config
Device(config)# snmp-server enable traps vtp
```

snmp-server enable traps bridge

To generate STP bridge MIB traps, use the **snmp-server enable traps bridge** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps bridge [**newroot**] [**topologychange**]
no snmp-server enable traps bridge [**newroot**] [**topologychange**]

Syntax Description		
newroot	(Optional) Enables SNMP STP bridge MIB new root traps.
topologychange	(Optional) Enables SNMP STP bridge MIB topology change traps.

Command Default The sending of bridge SNMP traps is disabled.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples This example shows how to send bridge new root traps to the NMS:

```
Device(config)# snmp-server enable traps bridge newroot
```

snmp-server enable traps bulkstat

To enable data-collection-MIB traps, use the **snmp-server enable traps bulkstat** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps bulkstat [**collection** | **transfer**]
no snmp-server enable traps bulkstat [**collection** | **transfer**]

Syntax Description		
collection	(Optional) Enables data-collection-MIB collection traps.	
transfer	(Optional) Enables data-collection-MIB transfer traps.	

Command Default   The sending of data-collection-MIB traps is disabled.

Command Modes   Global configuration

Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines   Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

> **Note**   Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples   This example shows how to generate data-collection-MIB collection traps:

```
Device(config)# snmp-server enable traps bulkstat collection
```

snmp-server enable traps call-home

To enable SNMP CISCO-CALLHOME-MIB traps, use the **snmp-server enable traps call-home** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps call-home [**message-send-fail** | **server-fail**]
no snmp-server enable traps call-home [**message-send-fail** | **server-fail**]

Syntax Description	**message-send-fail**	(Optional) Enables SNMP message-send-fail traps.
	server-fail	(Optional) Enables SNMP server-fail traps.

Command Default	The sending of SNMP CISCO-CALLHOME-MIB traps is disabled.

Command Modes	Global configuration

Command History	**Release**	**Modification**
	Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

✎

Note   Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples This example shows how to generate SNMP message-send-fail traps:

```
Device(config)# snmp-server enable traps call-home message-send-fail
```

snmp-server enable traps cef

To enable SNMP Cisco Express Forwarding (CEF) traps, use the **snmp-server enable traps cef** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]

no snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]

Syntax Description	**inconsistency**	(Optional) Enables SNMP CEF Inconsistency traps.
	peer-fib-state-change	(Optional) Enables SNMP CEF Peer FIB State change traps.
	peer-state-change	(Optional) Enables SNMP CEF Peer state change traps.
	resource-failure	(Optional) Enables SNMP CEF Resource Failure traps.

Command Default The sending of SNMP CEF traps is disabled.

Command Modes Global configuration

Command History	**Release**	**Modification**
	Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

> ✎
>
> **Note** Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples This example shows how to generate SNMP CEF inconsistency traps:

```
Device(config)# snmp-server enable traps cef inconsistency
```

snmp-server enable traps cpu

To enable CPU notifications, use the **snmp-server enable traps cpu** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps cpu [**threshold**]
no snmp-server enable traps cpu [**threshold**]

Syntax Description	**threshold**	(Optional) Enables CPU threshold notification.

Command Default	The sending of CPU notifications is disabled.

Command Modes	Global configuration

Command History	**Release**	**Modification**
	Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines
Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

> **Note** Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples
This example shows how to generate CPU threshold notifications:

```
Device(config)# snmp-server enable traps cpu threshold
```

snmp-server enable traps envmon

To enable SNMP environmental traps, use the **snmp-server enable traps envmon** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server   enable   traps   envmon [**status**]
no   snmp-server   enable   traps   envmon [**status**]

| Syntax Description | **status** | (Optional) Enables SNMP environmental status-change traps. |

Command Default The sending of environmental SNMP traps is disabled.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines In addition to enabling environmental status-change traps, the **snmp-server enable traps envmon status** command also enables traps for fan, power supply and temperature.

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples This example shows how to generate status-change traps:

```
Device(config)# snmp-server enable traps envmon status
```

snmp-server enable traps errdisable

To enable SNMP notifications of error-disabling, use the **snmp-server enable traps errdisable** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]
no snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]

Syntax Description	**notification-rate** *number-of-notifications*	(Optional) Specifies number of notifications per minute as the notification rate. Accepted values are from 0 to 10000.

Command Default The sending of SNMP notifications of error-disabling is disabled.

Command Modes Global configuration

Command History	**Release**	**Modification**
	Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples This example shows how to set the number SNMP notifications of error-disabling to 2:

Device(config)# **snmp-server enable traps errdisable notification-rate 2**

snmp-server enable traps flash

To enable SNMP flash notifications, use the **snmp-server enable traps flash** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps flash [**insertion**] [**removal**]
no snmp-server enable traps flash [**insertion**] [**removal**]

Syntax Description	**insertion**	(Optional) Enables SNMP flash insertion notifications.
	removal	(Optional) Enables SNMP flash removal notifications.

Command Default   The sending of SNMP flash notifications is disabled.

Command Modes   Global configuration

Command History	**Release**	**Modification**
	Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines   Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note	Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples   This example shows how to generate SNMP flash insertion notifications:

```
Device(config)# snmp-server enable traps flash insertion
```

snmp-server enable traps isis

To enable intermediate system-to-intermediate system (IS-IS) link-state routing protocol traps, use the **snmp-server enable traps isis** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps isis [**errors** | **state-change**]
no snmp-server enable traps isis [**errors** | **state-change**]

Syntax Description		
	errors	(Optional) Enables IS-IS error traps.
	state-change	(Optional) Enables IS-IS state change traps.

Command Default

The sending of IS-IS traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

> **Note** Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate IS-IS error traps:

```
Device(config)# snmp-server enable traps isis errors
```

snmp-server enable traps license

To enable license traps, use the **snmp-server enable traps license** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps license [**deploy**] [**error**] [**usage**]
no snmp-server enable traps license [**deploy**] [**error**] [**usage**]

Syntax Description

deploy	(Optional) Enables license deployment traps.
error	(Optional) Enables license error traps.
usage	(Optional) Enables license usage traps.

Command Default

The sending of license traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

> **Note** Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate license deployment traps:

```
Device(config)# snmp-server enable traps license deploy
```

snmp-server enable traps mac-notification

To enable SNMP MAC notification traps, use the **snmp-server enable traps mac-notification** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps mac-notification [**change**] [**move**] [**threshold**]
no snmp-server enable traps mac-notification [**change**] [**move**] [**threshold**]

Syntax Description	**change** (Optional) Enables SNMP MAC change traps.
	move (Optional) Enables SNMP MAC move traps.
	threshold (Optional) Enables SNMP MAC threshold traps.
Command Default	The sending of SNMP MAC notification traps is disabled.
Command Modes	Global configuration

Command History	**Release**	**Modification**
	Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

> **Note** Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples This example shows how to generate SNMP MAC notification change traps:

```
Device(config)# snmp-server enable traps mac-notification change
```

snmp-server enable traps ospf

To enable SNMP Open Shortest Path First (OSPF) traps, use the **snmp-server enable traps ospf** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time* *max-number-of-traps* | **retransmit** | **state-change**]
no snmp-server enable traps ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time* *max-number-of-traps* | **retransmit** | **state-change**]

Syntax Description		
	cisco-specific	(Optional) Enables Cisco-specific traps.
	errors	(Optional) Enables error traps.
	lsa	(Optional) Enables link-state advertisement (LSA) traps.
	rate-limit	(Optional) Enables rate-limit traps.
	rate-limit-time	(Optional) Specifies window of time in seconds for rate-limit traps. Accepted values are 2 to 60.
	max-number-of-traps	(Optional) Specifies maximum number of rate-limit traps to be sent in window time.
	retransmit	(Optional) Enables packet-retransmit traps.
	state-change	(Optional) Enables state-change traps.

Command Default	The sending of OSPF SNMP traps is disabled.

Command Modes	Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

> **Note** Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples This example shows how to enable LSA traps:

```
Device(config)# snmp-server enable traps ospf lsa
```

snmp-server enable traps pim

To enable SNMP Protocol-Independent Multicast (PIM) traps, use the **snmp-server enable traps pim** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps pim [**invalid-pim-message**] [**neighbor-change**] [**rp-mapping-change**]
no snmp-server enable traps pim [**invalid-pim-message**] [**neighbor-change**] [**rp-mapping-change**]

Syntax Description		
invalid-pim-message	(Optional) Enables invalid PIM message traps.
neighbor-change	(Optional) Enables PIM neighbor-change traps.
rp-mapping-change	(Optional) Enables rendezvous point (RP)-mapping change traps.

Command Default	The sending of PIM SNMP traps is disabled.
Command Modes	Global configuration

Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable invalid PIM message traps:

```
Device(config)# snmp-server enable traps pim invalid-pim-message
```

snmp-server enable traps port-security

To enable SNMP port security traps, use the **snmp-server enable traps port-security** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps port-security [**trap-rate** *value*]
no snmp-server enable traps port-security [**trap-rate** *value*]

Syntax Description	**trap-rate** *value*	(Optional) Sets the maximum number of port-security traps sent per second. The range is from 0 to 1000; the default is 0 (no limit imposed; a trap is sent at every occurrence).

Command Default   The sending of port security SNMP traps is disabled.

Command Modes   Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines   Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

> **Note**   Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples   This example shows how to enable port-security traps at a rate of 200 per second:

```
Device(config)# snmp-server enable traps port-security trap-rate 200
```

snmp-server enable traps power-ethernet

To enable SNMP power-over-Ethernet (PoE) traps, use the **snmp-server enable traps power-ethernet** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps power-ethernet {**group** *number* | **police**}
no snmp-server enable traps power-ethernet {**group** *number* | **police**}

Syntax Description	**group** *number*	Enables inline power group-based traps for the specified group number. Accepted values are from 1 to 9.
	police	Enables inline power policing traps.

Command Default   The sending of power-over-Ethernet SNMP traps is disabled.

Command Modes   Global configuration

Command History	**Release**	**Modification**
	Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines   Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note	Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples   This example shows how to enable power-over-Ethernet traps for group 1:

```
Device(config)# snmp-server enable traps poower-over-ethernet group 1
```

snmp-server enable traps snmp

To enable SNMP traps, use the **snmp-server enable traps snmp** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps snmp [**authentication**] [**coldstart**] [**linkdown**] [**linkup**] [**warmstart**]
no snmp-server enable traps snmp [**authentication**] [**coldstart**] [**linkdown**] [**linkup**] [**warmstart**]

Syntax Description	**authentication**	(Optional) Enables authentication traps.
	coldstart	(Optional) Enables cold start traps.
	linkdown	(Optional) Enables linkdown traps.
	linkup	(Optional) Enables linkup traps.
	warmstart	(Optional) Enables warmstart traps.

Command Default	The sending of SNMP traps is disabled.

Command Modes	Global configuration

Command History	**Release**	**Modification**
	Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines   Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

> **Note**   Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples   This example shows how to enable a warmstart SNMP trap:

```
Device(config)# snmp-server enable traps snmp warmstart
```

snmp-server enable traps storm-control

To enable SNMP storm-control trap parameters, use the **snmp-server enable traps storm-control** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps storm-control { **trap-rate** *number-of-minutes* }
no snmp-server enable traps storm-control { **trap-rate** }

Syntax Description	**trap-rate** *number-of-minutes*	(Optional) Specifies the SNMP storm-control trap rate in minutes. Accepted values are from 0 to 1000. The default is 0. Value 0 indicates that no limit is imposed and a trap is sent at every occurrence. When configured, **show run all** command output displays `no snmp-server enable traps storm-control`.

Command Default	The sending of SNMP storm-control trap parameters is disabled.

Command Modes	Global configuration

Command History	**Release**	**Modification**
	Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines
Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples
This example shows how to set the SNMP storm-control trap rate to 10 traps per minute:

```
Device(config)# snmp-server enable traps storm-control trap-rate 10
```

snmp-server enable traps stpx

To enable SNMP STPX MIB traps, use the **snmp-server enable traps stpx** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps stpx [**inconsistency**] [**loop-inconsistency**] [**root-inconsistency**]
no snmp-server enable traps stpx [**inconsistency**] [**loop-inconsistency**] [**root-inconsistency**]

Syntax Description		
inconsistency	(Optional) Enables SNMP STPX MIB inconsistency update traps.
loop-inconsistency	(Optional) Enables SNMP STPX MIB loop inconsistency update traps.
root-inconsistency	(Optional) Enables SNMP STPX MIB root inconsistency update traps.

Command Default   The sending of SNMP STPX MIB traps is disabled.

Command Modes   Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines   Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note   Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples   This example shows how to generate SNMP STPX MIB inconsistency update traps:

```
Device(config)# snmp-server enable traps stpx inconsistency
```

snmp-server enable traps transceiver

To enable SNMP transceiver traps, use the **snmp-server enable traps transceiver** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps transceiver {**all**}
no snmp-server enable traps transceiver {**all**}

Syntax Description	**all** (Optional) Enables all SNMP transceiver traps.

Command Default	The sending of SNMP transceiver traps is disabled.

Command Modes	Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines   Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

> **Note**   Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples   This example shows how to set all SNMP transceiver traps:

```
Device(config)# snmp-server enable traps transceiver all
```

snmp-server enable traps vrfmib

To allow SNMP vrfmib traps, use the **snmp-server enable traps vrfmib** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps vrfmib [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]
no snmp-server enable traps vrfmib [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]

Syntax Description

vnet-trunk-down	(Optional) Enables vrfmib trunk down traps.
vnet-trunk-up	(Optional) Enables vrfmib trunk up traps.
vrf-down	(Optional) Enables vrfmib vrf down traps.
vrf-up	(Optional) Enables vrfmib vrf up traps.

Command Default   The sending of SNMP vrfmib traps is disabled.

Command Modes   Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines   Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

> **Note**   Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples   This example shows how to generate vrfmib trunk down traps:

```
Device(config)# snmp-server enable traps vrfmib vnet-trunk-down
```

snmp-server enable traps vstack

To enable SNMP smart install traps, use the **snmp-server enable traps vstack** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps vstack [**addition**] [**failure**] [**lost**] [**operation**]
no snmp-server enable traps vstack [**addition**] [**failure**] [**lost**] [**operation**]

Syntax Description		
	addition	(Optional) Enables client added traps.
	failure	(Optional) Enables file upload and download failure traps.
	lost	(Optional) Enables client lost trap.
	operation	(Optional) Enables operation mode change traps.

Command Default

The sending of SNMP smart install traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

✎

Note   Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP Smart Install client-added traps:

```
Device(config)# snmp-server enable traps vstack addition
```

snmp-server engineID

To configure a name for either the local or remote copy of SNMP, use the **snmp-server engineID** command in global configuration mode.

snmp-server engineID {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}

Syntax Description		
local *engineid-string*	Specifies a 24-character ID string with the name of the copy of SNMP. You need not specify the entire 24-character engine ID if it has trailing zeros. Specify only the portion of the engine ID up to the point where only zeros remain in the value.
remote *ip-address*	Specifies the remote SNMP copy. Specify the *ip-address* of the device that contains the remote copy of SNMP.
udp-port *port-number*	(Optional) Specifies the User Datagram Protocol (UDP) port on the remote device. The default is 162.

Command Modes	Global configuration

Command History	Release	Modification
	Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines None

Examples

The following example configures a local engine ID of 123400000000000000000000:

```
Device(config)# snmp-server engineID local 1234
```

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*] [**match** {**exact** | **prefix**}] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] [{*acl-numberacl-name*}]]

no snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*]

Syntax Description	*group-name*	Name of the group.
	v1	Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.
	v2c	Specifies that the group is using the SNMPv2c security model.
		The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.
	v3	Specifies that the group is using the SNMPv3 security model.
		SMNPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.
	auth	Specifies authentication of a packet without encrypting it.
	noauth	Specifies no authentication of a packet.
	priv	Specifies authentication of a packet with encryption.
	context	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.
	context-name	(Optional) Context name.
	match	(Optional) Specifies an exact context match or matches only the context prefix.
	exact	(Optional) Matches the exact context.
	prefix	(Optional) Matches only the context prefix.
	read	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.
	read-view	(Optional) String of a maximum of 64 characters that is the name of the view.
		The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the **read** option is used to override this state.
	write	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.

write-view	(Optional) String of a maximum of 64 characters that is the name of the view.
	The default is that nothing is defined for the write view (that is, the null OID). You must configure write access.
notify	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap.
notify-view	(Optional) String of a maximum of 64 characters that is the name of the view.
	By default, nothing is defined for the notify view (that is, the null OID) until the **snmp-server host** command is configured. If a view is specified in the **snmp-server group** command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user).
	Cisco recommends that you let the software autogenerate the notify view. See the "Configuring Notify Views" section in this document.
access	(Optional) Specifies a standard access control list (ACL) to associate with the group.
ipv6	(Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list.
named-access-list	(Optional) Name of the IPv6 access list.
acl-number	(Optional) The *acl-number* argument is an integer from 1 to 99 that identifies a previously configured standard access list.
acl-name	(Optional) The *acl-name* argument is a string of a maximum of 64 characters that is the name of a previously configured standard access list.

Command Default No SNMP server groups are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines When a community string is configured internally, two groups with the name public are autogenerated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name public and a v2c group with the name public.

No default values exist for authentication or privacy algorithms when you configure the **snmp-server group** command. Also, no default passwords exist. For information about specifying a Message Digest 5 (MD5) password, see the documentation of the **snmp-server user** command.

Configuring Notify Views

The notify-view option is available for two reasons:

- If a group has a notify view that is set using SNMP, you may need to change the notify view.

- The **snmp-server host** command may have been configured before the **snmp-server group** command. In this case, you must either reconfigure the **snmp-server host** command, or specify the appropriate notify view.

Specifying a notify view when configuring an SNMP group is not recommended, for the following reasons:

- The **snmp-server host** command autogenerates a notify view for the user, and then adds it to the group associated with that user.

- Modifying the group's notify view will affect all users associated with that group.

Instead of specifying the notify view for a group as part of the **snmp-server group** command, use the following commands in the order specified:

1. **snmp-server user**—Configures an SNMP user.

2. **snmp-server group**—Configures an SNMP group, without adding a notify view .

3. **snmp-server host**—Autogenerates the notify view by specifying the recipient of a trap operation.

SNMP Contexts

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

Use this command with the **context** *context-name* keyword and argument to associate a read, write, or notify SNMP view with an SNMP context.

Create an SNMP Group

The following example shows how to create the SNMP server group "public," allowing read-only access for all objects to members of the standard named access list "lmnop":

```
Device(config)# snmp-server group public v2c access lmnop
```

Remove an SNMP Server Group

The following example shows how to remove the SNMP server group "public" from the configuration:

```
Device(config)# no snmp-server group public v2c
```

Associate an SNMP Server Group with Specified Views

The following example shows SNMP context "A" associated with the views in SNMPv2c group "GROUP1":

```
Device(config)# snmp-server context A
Device(config)# snmp mib community commA
```

```
Device(config)# snmp mib community-map commA context A target-list commAVpn
Device(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify viewB
```

Related Commands

Command	Description
show snmp group	Displays the names of groups on the device and the security model, the status of the different views, and the storage type of each group.
snmp mib community-map	Associates a SNMP community with an SNMP context, engine ID, security name, or VPN target list.
snmp-server host	Specifies the recipient of a SNMP notification operation.
snmp-server user	Configures a new user to a SNMP group.

snmp-server host

To specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** global configuration command on the device. Use the **no** form of this command to remove the specified host.

snmp-server host {*host-addr*} [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }

no snmp-server host {*host-addr*} [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }

Syntax Description		
host-addr	Name or Internet address of the host (the targeted recipient).	
vrf *vrf-instance*	(Optional) Specifies the virtual private network (VPN) routing instance and name for this host.	
informs | **traps**	(Optional) Sends SNMP traps or informs to this host.	
version 1 | **2c** | **3**	(Optional) Specifies the version of the SNMP used to send the traps. **1**—SNMPv1. This option is not available with informs. **2c**—SNMPv2C. **3**—SNMPv3. One of the authorization keywords (see next table row) must follow the Version 3 keyword.	
auth | **noauth** | **priv**	**auth** (Optional)—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. **noauth** (Default)—The noAuthNoPriv security level. This is the default if the **auth** | **noauth** | **priv** keyword choice is not specified. **priv** (Optional)—Enables Data Encryption Standard (DES) packet encryption (also called privacy).	
community-string	Password-like community string sent with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** global configuration command before using the **snmp-server host** command.	
	Note	The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the these keywords:

- **auth-framework**—Sends SNMP CISCO-AUTH-FRAMEWORK-MIB traps.

- **bridge**—Sends SNMP Spanning Tree Protocol (STP) bridge MIB traps.

- **bulkstat**—Sends Data-Collection-MIB Collection notification traps.

- **call-home**—Sends SNMP CISCO-CALLHOME-MIB traps.

- **cef**—Sends SNMP CEF traps.

- **config**—Sends SNMP configuration traps.

- **config-copy**—Sends SNMP config-copy traps.

- **config-ctid**—Sends SNMP config-ctid traps.

- **copy-config**—Sends SNMP copy configuration traps.

- **cpu**—Sends CPU notification traps.

- **cpu threshold**—Sends CPU threshold notification traps.

- **entity**—Sends SNMP entity traps.

- **envmon**—Sends environmental monitor traps.

- **errdisable**—Sends SNMP errdisable notification traps.

- **event-manager**—Sends SNMP Embedded Event Manager traps.

- **flash**—Sends SNMP FLASH notifications.

- **flowmon**—Sends SNMP flowmon notification traps.

- **ipmulticast**—Sends SNMP IP multicast routing traps.

- **ipsla**—Sends SNMP IP SLA traps.

- **license**—Sends license traps.

- **local-auth**—Sends SNMP local auth traps.

- **mac-notification**—Sends SNMP MAC notification traps.

- **pim**—Sends SNMP Protocol-Independent Multicast (PIM) traps.

- **power-ethernet**—Sends SNMP power Ethernet traps.

- **snmp**—Sends SNMP-type traps.

- **storm-control**—Sends SNMP storm-control traps.

- **stpx**—Sends SNMP STP extended MIB traps.

- **syslog**—Sends SNMP syslog traps.

- **transceiver**—Sends SNMP transceiver traps.

- **tty**—Sends TCP connection traps.

- **vlan-membership**— Sends SNMP VLAN membership traps.

- **vlancreate**—Sends SNMP VLAN-created traps.

- **vlandelete**—Sends SNMP VLAN-deleted traps.

- **vrfmib**—Sends SNMP vrfmib traps.

- **vtp**—Sends SNMP VLAN Trunking Protocol (VTP) traps.

- **wireless**—Sends wireless traps.

Command Default

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is Version 1.

If Version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.

Note	Though visible in the command-line help strings, the **fru-ctrl** keyword is not supported.

Command Modes   Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines   SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again, so that informs are more likely to reach their intended destinations.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Traps are also sent only once, but an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the device to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

If a local user is not associated with a remote host, the device does not send informs for the **auth** (authNoPriv) and the **priv** (authPriv) authentication levels.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable traps** global configuration command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

Examples   This example shows how to configure a unique SNMP community string named comaccess for traps and prevent SNMP polling access with this string through access-list 10:

```
Device(config)# snmp-server community comaccess ro 10
Device(config)# snmp-server host 172.20.2.160 comaccess
Device(config)# access-list 10 deny any
```

This example shows how to send the SNMP traps to the host specified by the name myhost.cisco.com. The community string is defined as comaccess:

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the device to send all traps to the host myhost.cisco.com by using the community string public:

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com public
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

snmp-server user

To configure a new user to a Simple Network Management Protocol (SNMP) group, use the **snmp-server user** command in global configuration mode. To remove a user from an SNMP group, use the **no** form of this command.

snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128** | **192** | **256**}} *privpassword*] {*acl-numberacl-name*}]

no snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128** | **192** | **256**}} *privpassword*] {*acl-numberacl-name*}]

Syntax Description

username	Name of the user on the host that connects to the agent.
group-name	Name of the group to which the user belongs.
remote	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.
host	(Optional) Name or IP address of the remote SNMP host.
udp-port	(Optional) Specifies the User Datagram Protocol (UDP) port number of the remote host.
port	(Optional) Integer value that identifies the UDP port. The default is 162.
vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
v1	Specifies that SNMPv1 should be used.
v2c	Specifies that SNMPv2c should be used.
v3	Specifies that the SNMPv3 security model should be used. Allows the use of the **encrypted** keyword or **auth** keyword or both.
encrypted	(Optional) Specifies whether the password appears in encrypted format.
auth	(Optional) Specifies which authentication level should be used.
md5	(Optional) Specifies the HMAC-MD5-96 authentication level.
sha	(Optional) Specifies the HMAC-SHA-96 authentication level.
auth-password	(Optional) String (not to exceed 64 characters) that enables the agent to receive packets from the host.
access	(Optional) Specifies an Access Control List (ACL) to be associated with this SNMP user.
ipv6	(Optional) Specifies an IPv6 named access list to be associated with this SNMP user.

nacl	(Optional) Name of the ACL. IPv4, IPv6, or both IPv4 and IPv6 access lists may be specified. If both are specified, the IPv6 named access list must appear first in the statement.
priv	(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.
des	(Optional) Specifies the use of the 56-bit Digital Encryption Standard (DES) algorithm for encryption.
3des	(Optional) Specifies the use of the 168-bit 3DES algorithm for encryption.
aes	(Optional) Specifies the use of the Advanced Encryption Standard (AES) algorithm for encryption.
128	(Optional) Specifies the use of a 128-bit AES algorithm for encryption.
192	(Optional) Specifies the use of a 192-bit AES algorithm for encryption.
256	(Optional) Specifies the use of a 256-bit AES algorithm for encryption.
privpassword	(Optional) String (not to exceed 64 characters) that specifies the privacy user password.
acl-number	(Optional) Integer in the range from 1 to 99 that specifies a standard access list of IP addresses.
acl-name	(Optional) String (not to exceed 64 characters) that is the name of a standard access list of IP addresses.

Command Default   See the table in the "Usage Guidelines" section for default behaviors for encryption, passwords, and access lists.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines   To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the **snmp-server engineID** command with the **remote** keyword. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.

For the *privpassword* and *auth-password*arguments, the minimum length is one character; the recommended length is at least eight characters, and should include both letters and numbers. The recommended maximum length is 64 characters.

The table below describes the default user characteristics for encryption, passwords, and access lists.

Table 1: snmp-server user Default Descriptions

Characteristic	Default
Access lists	Access from all IP access lists is permitted.
Encryption	Not present by default. The **encrypted** keyword is used to specify that the passwords are message digest algorithm 5 (MD5)digests and not text passwords.
Passwords	Assumed to be text strings.
Remote users	All users are assumed to be local to this SNMP engine unless you specify they are remote with the **remote** keyword.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For informs, the authoritative SNMP agent is the remote agent. You need to configure the remote agent's SNMP engine ID in the SNMP database before you can send proxy requests or informs to it.

Note   Changing the engine ID after configuring the SNMP user, does not allow to remove the user. To remove the user, you need to first reconfigure the SNMP user.

Working with Passwords and Digests

No default values exist for authentication or privacy algorithms when you configure the command. Also, no default passwords exist. The minimum length for a password is one character, although Cisco recommends using at least eight characters for security. The recommended maximum length of a password is 64 characters. If you forget a password, you cannot recover it and will need to reconfigure the user. You can specify either a plain-text password or a localized MD5 digest.

If you have the localized MD5 or Secure Hash Algorithm (SHA) digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hexadecimal values. Also, the digest should be exactly 16 octets long.

Examples

The following example shows how to add the user abcd to the SNMP server group named public. In this example, no access list is specified for the user, so the standard named access list applied to the group applies to the user.

```
Device(config)# snmp-server user abcd public v2c
```

The following example shows how to add the user abcd to the SNMP server group named public. In this example, access rules from the standard named access list qrst apply to the user.

```
Device(config)# snmp-server user abcd public v2c access qrst
```

In the following example, the plain-text password cisco123 is configured for the user abcd in the SNMP server group named public:

```
Device(config)# snmp-server user abcd public v3 auth md5 cisco123
```

When you enter a **show running-config** command, a line for this user will be displayed. To learn if this user has been added to the configuration, use the show snmp user command.

✎

Note   The **show running-config** command does not display any of the active SNMP users created in authPriv or authNoPriv mode, though it does display the users created in noAuthNoPriv mode. To display any active SNMPv3 users created in authPriv, authNoPrv, or noAuthNoPriv mode, use the **show snmp user** command.

If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hexadecimal values. Also, the digest should be exactly 16 octets long.

In the following example, the MD5 digest string is used instead of the plain-text password:

```
Device(config)# snmp-server user abcd public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

In the following example, the user abcd is removed from the SNMP server group named public:

```
Device(config)# no snmp-server user abcd public v2c
```

In the following example, the user abcd from the SNMP server group named public specifies the use of the 168-bit 3DES algorithm for privacy encryption with secure3des as the password.

```
Device(config)# snmp-server user abcd public priv v2c 3des secure3des
```

Related Commands

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.
show snmp user	Displays information on each SNMP username in the group username table.
snmp-server engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the device.

snmp-server view

To create or update a view entry, use the **snmp-server view** command in global configuration mode. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the **no**form of this command.

snmp-server view *view-name oid-tree* {**included** | **excluded**}
no snmp-server view *view-name*

Syntax Description		
	view-name	Label for the view record that you are updating or creating. The name is used to reference the record.
	oid-tree	Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
	included	Configures the OID (and subtree OIDs) specified in *oid-tree* argument to be included in the SNMP view.
	excluded	Configures the OID (and subtree OIDs) specified in *oid-tree* argument to be explicitly excluded from the SNMP view.

Command Default   No view entry exists.

Command Modes

Global configuration

Command History	Release	Modification
	Cisco IOS XE Fuji 16.8.1a	This command was introduced.

Usage Guidelines   Other SNMP commands require an SMP view as an argument. You use this command to create a view to be used as arguments for other commands.

Two standard predefined views can be used when a view is required, instead of defining a view. One is *everything*, which indicates that the user can see all objects. The other is *restricted,*which indicates that the user can see three groups: system, snmpStats, and snmpParties. The predefined views are described in RFC 1447.

The first **snmp-server** command that you enter enables SNMP on your routing device.

Examples   The following example creates a view that includes all objects in the MIB-II subtree:

```
snmp-server view mib2 mib-2 included
```

The following example creates a view that includes all objects in the MIB-II system group and all objects in the Cisco enterprise MIB:

```
snmp-server view root_view system included
snmp-server view root_view cisco included
```

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group:

```
snmp-server view agon system included
snmp-server view agon system.7 excluded
snmp-server view agon ifEntry.*.1 included
```

In the following example, the USM, VACM, and Community MIBs are explicitly included in the view "test" with all other MIBs under the root parent "internet":

```
! -- include all MIBs under the parent tree "internet"
snmp-server view test internet included
! -- include snmpUsmMIB
snmp-server view test 1.3.6.1.6.3.15 included
! -- include snmpVacmMIB
snmp-server view test 1.3.6.1.6.3.16 included
! -- exclude snmpCommunityMIB
snmp-server view test 1.3.6.1.6.3.18 excluded
```

Related Commands	**Command**	**Description**
	snmp-server community	Sets up the community access string to permit access to the SNMP protocol.
	snmp-server manager	Starts the SNMP manager process.

switchport mode access

To sets the interface as a nontrunking nontagged single-VLAN Ethernet interface , use the **switchport mode access** command in template configuration mode. Use the **no** form of this command to return to the default setting.

switchport mode access
no switchport mode access

| Syntax Description | **switchport mode access** Sets the interface as a nontrunking nontagged single-VLAN Ethernet interface. |

Command Default An access port can carry traffic in one VLAN only. By default, an access port carries traffic for VLAN1.

Command Modes Template configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples This example shows how to set a single-VLAN interface

```
Device(config-template)# switchport mode access
```

switchport voice vlan

To specify to forward all voice traffic through the specified VLAN, use the **switchport voice vlan** command in template configuration mode. Use the **no** form of this command to return to the default setting.

switchport voice vlan*vlan_id*
no switchport voice vlan

Syntax Description

switchport voice vlan*vlan_id*	Specifies to forward all voice traffic through the specified VLAN.

Command Default   You can specify a value from 1 to 4094.

Command Modes   Template configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples   This example shows how to specify to forward all voice traffic through the specified VLAN.

```
Device(config-template)# switchport voice vlan 20
```