Network Management

debug event manager auto-deploy

To enable the debugging of Embedded Event Manager (EEM) auto-deploy policies, use the **debug event manager auto-deploy** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

debug event manager auto-deploy {**common** | **parser** | **schedule**}
no debug event manager auto-deploy {**common** | **parser** | **schedule**}

Syntax Description

common	Enables the logging of EEM auto-deploy infrastructure-related debugs.
parser	Enables the logging of the manifest file parsing debugs.
schedule	Enables the logging of EEM policy provisioning debugs.

Command Default

Debugs are not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Example

The following example shows how to enable schedule logs:

```
Device# debug event manager auto-deploy schedule

*Jul 26 16:45:22.731 IST: [fadpa]
*Jul 26 16:45:22.731 IST: [fadec]
*Jul 26 16:45:22.733 IST: fadpa: CLI execution is done
*Jul 26 16:45:22.733 IST:
*Jul 26 16:45:22.733 IST: Provisioned ENV A.ENV policy

*Jul 26 16:45:22.734 IST: [fadpl]
*Jul 26 16:45:22.734 IST: [fadv]
*Jul 26 16:45:22.734 IST: Successfully provisioned env vars

*Jul 26 16:45:22.734 IST: [fadpl]
*Jul 26 16:45:22.734 IST: [fadv]
*Jul 26 16:45:22.734 IST: [fadpfp]
*Jul 26 16:45:22.735 IST: [fadfxr]
*Jul 26 16:45:22.735 IST: [fadft]
*Jul 26 16:45:22.790 IST:
*Jul 26 16:45:22.790 IST: Downloaded APP policy
```

Related Commands

Command	Description
event manager auto-deploy	Configures an EEM auto-deployment profile.

default

To set policy provisioning commands to the default state, use the default command in auto-deploy configuration mode.

default {**enable** | **exit** | **log-url** | **manifest format xml url** | **retry count** *retry-count* **interval** *interval-duration* | **schedule start-in hours** *hours* **minutes** *minutes* {**oneshot** | **recurring** {**days** *days* | **hours** *hours*}} | **window** *minutes*}

Syntax Description

enable	Enables the profile.
exit	Exits auto-deploy configuration mode.
log-url	Sets the location where the log file for policy provisioning must be stored.
manifest format xml url	Sets the manifest file format, and the location from where the manifest file must be downloaded.
retry count *retry-count* **interval** *interval-duration*	Sets the number of retries to transfer a file, if the file transfer is not successful.
schedule start-in hours *hours* **minutes** *minutes*	Schedules policy provisioning after the specified time.
oneshot	Schedules policy provisioning.
recurring days *days* **hours** *hours*	Schedules recurring policy provisioning during the specified time.
window *minutes*	Sets a random time for profile provisioning to be triggered. The window duration is added to the scheduled start-in time, and policy provisioning will happen any time between the scheduled start-in time and the configured window duration.

Command Default

Auto-depoly commands are not enabled.

Command Modes

Auto-deploy configuration mode (config-auto-deploy)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Example

The following example shows how to set a command to its default:

```
Device(config)# event manager auto-deploy name deploy1
Device(auto-deploy)# default retry count 2 interval 3
```

Related Commands

Command	Description
event-manager auto-deploy	Configures an EEM auto-deployment profile.

description (ERSPAN)

To describe an Encapsulated Remote Switched Port Analyzer (ERSPAN) source session, use the **description** command in ERSPAN monitor source session configuration mode. To remove a description, use the **no** form of this command.

description *description*
no description

Syntax Description

description	Describes the properties for this session.

Command Default

Description is not configured.

Command Modes

ERSPAN monitor source session configuration mode (config-mon-erspan-src)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

The *description* argument can be up to 240 characters.

Examples

The following example shows how to describe an ERSPAN source session:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# description source1
```

Related Commands

Command	Description
monitor session type erspan-source	Configures a local ERSPAN source session.

destination (ERSPAN)

To configure an Encapsulated Remote Switched Port Analyzer (ERSPAN) source session destination and specify destination properties, use the **destination** command in ERSPAN monitor source session configuration mode. To remove a destination session, use the **no** form of this command.

destination
no destination

Syntax Description

This command has no arguments or keywords.

Command Default

A source session destination is not configured.

Command Modes

ERSPAN monitor source session configuration mode (config-mon-erspan-src)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

ERSPAN traffic is GRE-encapsulated SPAN traffic that can only be processed by an ERSPAN destination session.

All ERSPAN source session (maximum 8) destination IP address need not be same. Enter the **ip address** command to configure the IP address for the ERSPAN destination sessions.

The ERSPAN source session destination IP address, which is configured on an interface on the destination switch, is the source of traffic that an ERSPAN destination session sends to destination ports. Configure the same address in both the source and destination sessions with the **ip address** command.

Examples

The following example shows how to configure an ERSPAN source session destination and enter the ERSPAN monitor destination session configuration mode to specify the destination properties:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)#ip address 10.1.1.1
Switch(config-mon-erspan-src-dst)#
```

The following sample output from the **show monitor session all** displays different IP addresses for source session destinations:

```
Switch# show monitor session all

Session 1
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session1
Destination IP Address : 10.1.1.1


Session 2
---------
Type : ERSPAN Source Session
```

```
Status : Admin Disabled
Description : session2
Destination IP Address : 192.0.2.1


Session 3
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session3
Destination IP Address : 198.51.100.1

Session 4
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session4
Destination IP Address : 203.0.113.1


Session 5
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session5
Destination IP Address : 209.165.200.225
```

Related Commands

Command	Description
erspan-id	Configures the ID used by the destination session to identify the ERSPAN traffic.
ip ttl	Configures TTL values for packets in the ERSPAN traffic.
monitor session type erspan-source	Configures a local ERSPAN source session.
origin	Configures an IP address used as the source of the ERSPAN traffic.

enable

To enable the Embedded Event Manager (EEM) profile, use the **enable** command in auto-deploy configuration mode. To disable the EEM profile, use the **no** form of this command.

enable
no enable

This command has no arguments or keywords.

Command Default

EEM profiles are not enabled.

Command Modes

Auto-deploy configuration (config-auto-deploy)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

Unless the configured profile is enabled, that profile will not be active, and policy provisioning will not start.

Example

The following example shows how to enable an EEM profile:

```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# enable
```

Related Commands

Command	Description
event-manager auto-deploy	Configures an EEM auto-deployment profile.

erspan-id

To configure the ID used by the destination session to identify the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic, use the **erspan-id** command in ERSPAN monitor destination session configuration mode. To remove the configuration, use the **no** form of this command.

erspan-id *erspan-ID*
no erspan-id *erspan-ID*

Syntax Description

erspan-id	ERSPAN ID used by the destination session. Valid values are from 1 to 1023.

Command Default

ERSPAN IDs for destination sessions are not configured.

Command Modes

ERSPAN monitor destination session configuration mode (config-mon-erspan-src-dst)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

The following example shows how to configure an ERSPAN ID for a destination session:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# erspan-id 3
```

Related Commands

Command	Description
destination	Configures an ERSPAN destination session and specifies destination properties.
monitor session type erspan-source	Configures a local ERSPAN source session.

event manager auto-deploy

To configure an Embedded Event Manager (EEM) auto-deployment profile, use the **event manager auto-deploy** command in global configuration mode. To disable the configuration, use the **no** form of this command.

event manager auto-deploy name *profile-name*
no event manager auto-deploy name *profile-name*

Syntax Description

name *profile-name*	Specifies a name for the auto-deployment profile.

Command Default

Default profile is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

After you configure this command, the mode changes to auto-deploy configuration mode. Auto-deployment configuration settings can be configure in this mode. At any given point of time, more than one profile cannot be enabled.

Example

The following example show how to configure the auto-deployment of an EEM profile:

```
Device(config)# event manager auto-deploy name deploy1
```

Related Commands

Command	Description
show event-manager auto-deploy summary	Displays information about auto-deployed profiles.

event manager auto-deploy start

To trigger the Embedded Event Manager (EEM) auto-deployment instantly, and to start the policy processing, use the **event manager auto-deploy start** command in privileged EXEC mode.

event manager auto-deploy start name *profile-name* {**now** | **window** *duration*}

Syntax Description

name *profile-name*	Specifies a name for the auto-deployment profile.
now	Species that the EEM auto-deployment should start immediately.
window *duration*	Specifies that the EEM auto-deployment should start at any random time of the specified window duration. Valid values for the *duration* argument are 5 to 30 minutes.

Command Default

EEM auto-deployment is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Example

The following example shows how to start policy processing immediately:

```
Device# event manager auto-deploy start name deploy1 now
```

The following example shows how to start policy processing at any time within the specified window duration:

```
Device# event manager auto-deploy start name deploy1 window 20
```

filter (ERSPAN)

To configure the Encapsulated Remote Switched Port Analyzer (ERSPAN) source VLAN filtering when the ERSPAN source is a trunk port, use the **filter** command in ERSPAN monitor source session configuration mode. To remove the configuration, use the **no** form of this command.

filter {**ip access-group** {*standard-access-list extended-access-list acl-name*} | **ipv6 access-group** *acl-name* | **mac access-group** *acl-name* | **vlan** *vlan-id* [{**,**}] [{**-**}]}
no filter {**ip** [{**access-group** | [{*standard-access-list extended-access-list acl-name*}]}] | **ipv6** [{**access-group**}] | **mac** [{**access-group**}] | **vlan** *vlan-id* [{**,**}] [{**-**}]}

Syntax Description

ip	Specifies the IP access control rules.
access-group	Specifies an access control group.
standard-access-list	Standard IP access list.
extended-access-list	Extended IP access list.
acl-name	Access list name.
ipv6	Specifies the IPv6 access control rules.
mac	Specifies the media access control (MAC) rules.
vlan *vlan-ID*	Specifies the ERSPAN source VLAN. Valid values are from 1 to 4094.
,	(Optional) Specifies another VLAN.
-	(Optional) Specifies a range of VLANs.

Command Default

Source VLAN filtering is not configured.

Command Modes

ERSPAN monitor source session configuration mode (config-mon-erspan-src)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

You cannot include source VLANs and filter VLANs in the same session.

When you configure the **filter** command on a monitored trunk interface, only traffic on that set of specified VLANs is monitored.

Examples

The following example shows how to configure source VLAN filtering:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# filter vlan 3
```

Related Commands

Command	Description
monitor session type erspan-source	Configures a local ERSPAN source session.

ip ttl (ERSPAN)

To configure Time to Live (TTL) values for packets in the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic, use the **ip ttl** command in ERSPAN monitor destination session configuration mode. To remove the TTL values, use the **no** form of this command,

ip ttl *ttl-value*
no ip ttl *ttl-value*

Syntax Description

ttl-value	TTL value. Valid values are from 2 to 255.

Command Default

TTL value is set as 255.

Command Modes

ERSPAN monitor destination session configuration mode (config-mon-erspan-src-dst)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

The following example shows how to configure TTL value for ERSPAN traffic:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# ip ttl 32
```

Related Commands

Command	Description
destination	Configures an ERSPAN destination session and specifies destination properties.
monitor session type erspan-source	Configures a local ERSPAN source session.

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 devices 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 3.2SE	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
```

log-url

To specify the location where provisioning logs must be stored, use the **log-url** command in auto-deploy configuration mode. To remove the configuration, use the **no** form of this command.

log-url *URL*
no log-url

Syntax Description

URL	Location for status logs.

Command Default

URL for status logs is not specified.

Command Modes

Auto-deploy configuration (config-auto-deploy)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

The log URL can be configured either in the manifest file or by using the **log-url** command. If the log URL is configured by both ways, the log URL in the manifest file is used. Valid values for the *URL* argument are the following:

- flash:
- ftp:
- http:
- https:
- tftp:

Example

The following example shows how to specify an URL to log status logs:

```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# log-url tftp://10.106.16.20/folder1/EEM
```

Related Commands

Command	Description
event-manager auto-deploy	Configures an EEM auto-deployment profile.

manifest format

To specify the manifest file format and location details, use the **manifest format** command in auto-deploy configuration mode. To remove the configuration, use the **no** form of this command.

manifest format xml url *URL*
no manifest format xml url

Syntax Description

xml	Specifies the manifest file format as XML.
url *URL*	Specifies the location to store manifest files.

Command Default

Manifest file details are not specified.

Command Modes

Auto-deploy configuration (config-auto-deploy)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

Valid values for the *URL* argument are the following:

- flash:
- ftp:
- http:
- https:
- tftp:

Example

The following example shows how to specify the manifest file format and location details:

```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# manifest format xml url tftp://10.106.16.20/folder1/123.xml
```

Related Commands

Command	Description
event-manager auto-deploy	Configures an EEM auto-deployment profile.

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:
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 3.3SE	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.

Multiple capture points can be defined, but only one can be active at a time. In other words, you have to stop one before you can start the other.

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 unless you are using a CAPWAP tunneling attachment point in your capture point.

If you are using CAPWAP tunneling attachment points in your capture point, you cannot use core filters.

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
```

To define a capture point with a CAPWAP attachment point:

```
Device# show capwap summary

CAPWAP Tunnels General Statistics:
  Number of Capwap Data Tunnels       = 1
  Number of Capwap Mobility Tunnels   = 0
  Number of Capwap Multicast Tunnels  = 0


Name   APName                          Type PhyPortIf Mode      McastIf
------ ------------------------------- ---- --------- --------- -------
Ca0    AP442b.03a9.6715                data Gi3/0/6   unicast   -


Name   SrcIP           SrcPort DestIP          DstPort DtlsEn MTU   Xact
------ --------------- ------- --------------- ------- ------ ----- ----
Ca0    10.10.14.32     5247    10.10.14.2      38514   No     1449  0

Device# monitor capture mycap interface capwap 0 both
Device# monitor capture mycap file location flash:mycap.pcap
Device# monitor capture mycap file buffer-size 1
Device# monitor capture mycap start

*Aug 20 11:02:21.983: %BUFCAP-6-ENABLE: Capture Point mycap enabled.on

Device# show monitor capture mycap parameter
```

```
   monitor capture mycap interface capwap  0 in
   monitor capture mycap interface capwap  0 out
   monitor capture mycap file location flash:mycap.pcap buffer-size 1
Device#
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)
Device#
Device# show monitor capture file flash:mycap.pcap
 1   0.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 2   0.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 3   2.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 4   2.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 5   3.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 6   4.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 7   4.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 8   5.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 9   5.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
10   6.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
11   8.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
12   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
13   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
14   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
15   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
16   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
17   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
18   9.236987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
19  10.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
20  10.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
21  12.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
```

```
22  12.239993   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
23  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
24  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
25  12.250994   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
26  12.256990   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
27  12.262987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
28  12.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=........
29  12.802012   10.10.14.3 -> 10.10.14.255 NBNS Name query NB WPAD.<00>
30  13.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=........
```

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 3.3SE	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 clear

To clears the monitor capture (WireShark) buffer, use the **monitor capture clear** command in privileged EXEC mode.

monitor capture {*capture-name*} **clear**

Syntax Description

capture-name	The name of the capture whose buffer is to be cleared.

Command Default

The buffer content is not cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Use the **monitor capture clear** command either during capture or after the capture has stopped either because one or more end conditions has been met, or you entered the **monitor capture stop** command. If you enter the **monitor capture clear** command after the capture has stopped, the **monitor capture export** command that is used to store the contents of the captured packets in a file will have no impact because the buffer has no captured packets.

If you have more than one capture that is storing packets in a buffer, clear the buffer before starting a new capture to avoid memory loss.

Example

To clear the buffer contents for capture mycap:

```
Device#  monitor capture mycap clear
```

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 • (usbflash0:)— USB drive

Command Default

The captured packets are not stored.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	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:

```
Device# monitor capture mycap export flash:mycap.pcap
```

monitor capture file

To configure monitor capture (WireShark) storage file attributes, use the **monitor capture file** command in privileged EXEC mode. To remove a storage file attribute, use the **no** form of this command.

monitor capture {*capture-name*} **file**{ [**buffer-size** *temp-buffer-size*] [**location** *file-location* **:** *file-name*] [**ring** *number-of-ring-files*] [**size** *total-size*] }
no monitor capture {*capture-name*} **file**{ [**buffer-size**] [**location**] [**ring**] [**size**] }

Syntax Description

capture-name	The name of the capture to be modified.
buffer-size *temp-buffer-size*	(Optional) Specifies the size of the temporary buffer. The range for *temp-buffer-size* is 1 to 100 MB. This is specified to reduce packet loss.
location *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 • (usbflash0:)— USB drive
ring *number-of-ring-files*	(Optional) Specifies that the capture is to be stored in a circular file chain and the number of files in the file ring.
size *total-size*	(Optional) Specifies the total size of the capture files.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Use the **monitor capture file** command only when the storage destination is a file. The file may be stored either remotely or locally. Use this command 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 specify that the storage file name is mycap.pcap, stored on a flash drive:

```
Device# monitor capture mycap file location flash:mycap.pcap
```

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 3.3SE	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 match

Note Do not use this command when capturing a CAPWAP tunnel. Also, when control plane and CAPWAP tunnels are mixed, this command will have no effect.

To define an explicit inline core filter for a monitor (Wireshark) capture, use the **monitor capture match** command in privileged EXEC mode. To remove this filter, use the **no** form of this command.

monitor capture {*capture-name*} **match** {**any** | **mac** *mac-match-string* | **ipv4** {**any** | **host** | **protocol**}{**any** | **host**} | **ipv6** {**any** | **host** | **protocol**}{**any** | **host**}}
no monitor capture {*capture-name*} **match**

Syntax Description

capture-name	The name of the capture to be assigned a core filter.
any	Specifies all packets.
mac *mac-match-string*	Specifies a Layer 2 packet.
ipv4	Specifies IPv4 packets.
host	Specifies the host.
protocol	Specifies the protocol.
ipv6	Specifies IPv6 packets.

Command Default

A core filter is not configured.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Examples

To define a capture point and the core filter for the capture point that matches to any IP version 4 packets on the source or destination:

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

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 3.3SE	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 3.3SE	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

To create a new Ethernet Switched Port Analyzer (SPAN) or a Remote Switched Port Analyzer (RSPAN) session configuration for analyzing traffic between ports or add to an existing session configuration, use the **monitor session** global configuration command. To clear SPAN or RSPAN sessions, use the **no** form of this command.

monitor session *session-number* {**destination** | **filter** | **source**}
no monitor session {*session-number* [**destination** | **filter** | **source**] | **all** | **local** | **range** *session-range* | **remote**}

Syntax Description

session-number	The session number identified with the SPAN or RSPAN session. The range is 1 to 66.
all	Clears all monitor sessions.
local	Clears all local monitor sessions.
range *session-range*	Clears monitor sessions in the specified range.
remote	Clears all remote monitor sessions.

Command Default

No monitor sessions are configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch or switch stack.

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.

Example

This example shows how to create a local SPAN session 1 to monitor traffic on Po13 (an EtherChannel port) and limit SPAN traffic in the session only to VLAN 1281. Egress traffic replicates the source; ingress forwarding is not enabled.

```
Device(config)# monitor session 1 source interface Po13
Device(config)# monitor session 1 filter vlan 1281
Device(config)# monitor session 1 destination interface GigabitEthernet2/0/36 encapsulation
 replicate
Device(config)# monitor session 1 destination interface GigabitEthernet3/0/36 encapsulation
 replicate
```

The following is the output of a **show monitor session all** command after completing these setup instructions:

```
Device# show monitor session all

Session 1
---------
Type                     : Local Session
Source Ports             :
    Both                 : Po13
Destination Ports      : Gi2/0/36,Gi3/0/36
    Encapsulation      : Replicate
          Ingress      : Disabled
Filter VLANs           : 1281
...
```

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	The session number identified with the SPAN or RSPAN session. The range is 1 to 66.
interface *interface-id*	Specifies the destination or 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 128.
,	(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.
encapsulation replicate	(Optional) Specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged). These keywords are valid only for local SPAN. For RSPAN, the RSPAN VLAN ID overwrites the original VLAN ID; therefore, packets are always sent untagged. The **encapsulation** options are ignored with the **no** form of the command.
encapsulation dot1q	(Optional) Specifies that the destination interface accepts the source interface incoming packets with IEEE 802.1Q encapsulation. These keywords are valid only for local SPAN. For RSPAN, the RSPAN VLAN ID overwrites the original VLAN ID; therefore, packets are always sent untagged. The **encapsulation** options are ignored with the **no** form of the command.

ingress	Enables ingress traffic forwarding.
dot1q	(Optional) Accepts incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.
untagged	(Optional) Accepts incoming packets with untagged encapsulation with the specified VLAN as the default VLAN.
isl	Specifies ingress forwarding using ISL encapsulation.
remote	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*	Sets the default VLAN for ingress traffic when used with only the **ingress** keyword.

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 3.2SE	This command was introduced.

Usage Guidelines

You can set a combined maximum of 8 local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch or switch stack.

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	The session number identified with the SPAN or RSPAN session. The range is 1 to 66.
vlan *vlan-id*	Specifies a list of VLANs as filters on trunk source ports to limit SPAN source traffic to specific VLANs. The *vlan-id* range is 1 to 4094.
,	(Optional) Specifies a series of VLANs, or separates a range of VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specifies a range of VLANs. Enter a space before and after the hyphen.

Command Default

No monitor sessions are configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch or switch stack.

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:

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
Switch(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	The session number identified with the SPAN or RSPAN session. The range is 1 to 66.
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 3.2SE	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.

You can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch or switch stack.

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
```

monitor session type erspan-source

To configure a local Encapsulated Remote Switched Port Analyzer (ERSPAN) source session, use the **monitor session type erspan-source** command in global configuration mode. To remove the ERSPAN configuration, use the **no** form of this command.

monitor session *span-session-number* **type erspan-source**
no monitor session *span-session-number* **type erspan-source**

Syntax Description

span-session-number	Number of the local ERSPAN session. Valid values are from 1 to 66.

Command Default

ERSPAN source session is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

The *span-session-number* and the session type (configured by the *erspan-source* keyword) cannot be changed once configured. Use the **no** form of this command to remove the session and then re-create the session with a new session ID or a new session type.

The ERSPAN source session destination IP address, which must be configured on an interface on the destination switch, is the source of traffic that an ERSPAN destination session sends to the destination ports. You can configure the same address in both the source and destination sessions with the **ip address** command in ERSPAN monitor destination session configuration mode.

The ERSPAN ID differentiates the ERSPAN traffic arriving at the same destination IP address from different ERSPAN source sessions.

The maximum local ERSPAN source session limit is 8.

Examples

The following example shows how to configure an ERSPAN source session number:

```
Switch(config)# monitor session 55 type erspan-source
Switch(config-mon-erspan-src)#
```

Related Commands

Command	Description
monitor session type	Creates an ERSPAN source session number or enters the ERSPAN session configuration mode for the session.
show capability feature monitor	Displays information about monitor features.
show monitor session	Displays information about the ERSPAN, SPAN, and RSPAN sessions.

origin

To configure the IP address used as the source of the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic, use the **origin** command in ERSPAN monitor destination session configuration mode. To remove the configuration, use the **no** form of this command.

origin *ip-address*
no origin *ip-address*

Syntax Description

ip-address	Specifies the ERSPAN source session destination IP address.

Command Default

Source IP address is not configured.

Command Modes

ERSPAN monitor destination session configuration mode (config-mon-erspan-src-dst)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

ERSPAN source session on a switch can use different source IP addresses using the **origin** command.

Examples

The following example shows how to configure an IP address for an ERSPAN source session:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# origin ip-address 203.0.113.2
```

The following sample output from the **show monitor session all** command displays ERSPAN source sessions with different source IP addresses:

```
Session 3
---------
Type : ERSPAN Source Session
Status : Admin Enabled
Source Ports :
Both : Gi1/0/13
Destination IP Address : 10.10.10.10
Origin IP Address : 10.10.10.10


Session 4
---------
Type : ERSPAN Source Session
Status : Admin Enabled
Destination IP Address : 192.0.2.1
Origin IP Address : 203.0.113.2
```

Related Commands

Command	Description
destination	Configures an ERSPAN destination session and specifies destination properties.
monitor session type erspan-source	Configures a local ERSPAN source session.

retry count

To set the number of retries to transfer a file, if the file transfer is not successful, use the **retry count** command in auto-deploy configuration mode. To remove the configuration, use the **no** form of this command.

retry count *retry-count* **interval** *interval-duration*
no retry count *retry-count* **interval** *interval-duration*

Syntax Description

retry-count	Number of retries to transfer a file, if file transfer is not successful. Valid values are from 1 to 3.
interval *interval-duration*	Specifies the interval between retries. Valid values are from 2 to 4 minutes.

Command Default

The default is zero.

Command Modes

Auto-deploy configuration (config-auto-deploy)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Example

The following example shows how to set the retry count for files that are not tranferred successfully:

```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# retry count 3 interval 3
```

Related Commands

Command	Description
event-manager auto-deploy	Configures an EEM auto-deployment profile.

schedule start-in

To schedule the provisioning of policies, use the **schedule start-in** command in auto-deploy configuration mode. To remove the scheduling, use the **no** form of this command.

schedule start-in hours *hours* **minutes** *minutes* {**oneshot** | **recurring** {**days** *days* | **hours** *hours*}}
no schedule start-in hours *hours* **minutes** *minutes* {**oneshot** | **recurring** {**days** *days* | **hours** *hours*}}

Syntax Description

hours *hours*	Specifies the time in hours, when the policy provisioning should start. Valid values are from 0 to 23.
minutes *minutes*	Specifies the time in minutes, when the policy provisioning should start. Valid values are from 0 to 59.
oneshot	Schedules the policy provisioning to be done only once.
recurring	Schedules the policy provisioning repeatedly.
days *days*	Specifies the time in days, when the policy provisioning should repeat. Valid values are from 1 to 30.
hours *hours*	Specifies the time in hours, when the policy provisioning should repeat. Valid values are from 12 to 168.

Command Default

Scheduling of policy provisioning is not enabled.

Command Modes

Auto-deploy configuration (config-auto-deploy)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

Example

The following example shows how to schedule policy provisioning to be done only once:

```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# schedule start-in hours 2 minutes 30 oneshot
```

The following example shows how to schedule a recurring policy provisioning:

```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# schedule start-in hours 2 minutes 30 recurring days 2
```

Related Commands

Command	Description
event-manager auto-deploy	Configures an EEM auto-deployment profile.

show capability feature monitor

To display information about monitor features, use the **show capability feature monitor** command in privileged EXEC mode.

show capability feature monitor {**erspan-destination** | **erspan-source**}

Syntax Description

erspan-destination	Displays information about the configured Encapsulated Remote Switched Port Analyzer (ERSPAN) source sessions.
erspan-source	Displays all the configured global built-in templates.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

The following is sample output from the **show capability feature monitor erspan-source** command:

```
Switch# show capability feature monitor erspan-source

ERSPAN Source Session Supported: true
No of Rx ERSPAN source session: 8
No of Tx ERSPAN source session: 8
ERSPAN Header Type supported: II
ACL filter Supported: true
Fragmentation Supported: true
Truncation Supported: false
Sequence number Supported: false
QOS Supported: true
```

The following is sample output from the **show capability feature monitor erspan-destination** command:

```
Switch# show capability feature monitor erspan-destination

ERSPAN Destination Session Supported: false
```

Related Commands

Command	Description
monitor session type erspan-source	Creates an ERSPAN source session number or enters the ERSPAN session configuration mode for the session.

show event manager auto-deploy summary

To display a summary of the auto-deployment profile information, use the **show event manager auto-deploy summary** command in privileged EXEC mode.

show event manager auto-deploy summary

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was modified.

Usage Guidelines

Example

The following is sample output from the **show event manager auto-deploy summary** command:

```
Device# show event manager auto-deploy summary

EEM Auto-Deploy Profile details:

    Profile Name  : test
    Status        : Enabled
    Running       : Yes
    Status Syslog : No
    Schedule      : start in 0 hours 5 mins oneshot
    Window        : 5
    Manifest URL  : tftp://10.106.16.20/folder1/123.xml
    Log URL       : tftp://10.106.16.20/folder1/EEM
```

The table below lists the significant fields shown in the display.

Table 1: show event manager auto-deploy summary Field Descriptions

Field	Description
Profile Name	Name specified for the profile.
Status	Status of the profile provisioning; whether enabled or disabled.
Running	The enabled profile is running or not.
Schedule	Policy provisioning schedule
Window	Window duration added to the policy provisioning time. Policy provisioning will happen at a random time, between the policy provisioning time and the configured window duration in minutes.
Manifest URL	Location of the manifest file.

Field	Description
Log URL	Location where the debug logs are stored.

Related Commands

Command	Description
event-manager auto-deploy	Configures an EEM auto-deployment profile.

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 3.2SE	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	The session number identified with the SPAN or RSPAN session. The range is 1 to 66.
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 3.2SE	This command was introduced.

Usage Guidelines

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

Maximum number of SPAN source sessions: 2 (applies to source and local sessions)

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 file** 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 3.3SE	This command was introduced.

Usage Guidelines

none

Example

To display the capture for a capture called mycap:

```
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 monitor session

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

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

Syntax Description

session_number	The session number identified with the SPAN or RSPAN session. The range is 1 to 68. However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions, and the range is 1 to 66.
all	Displays all SPAN sessions.
erspan-source	Displays only source ERSPAN sessions.
local	Displays only local SPAN sessions.
range *list*	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	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 3.2SE	This command was introduced.

Usage Guidelines

The maximum local ERSPAN source session limit is 8.

Examples

The following is sample output from the **show monitor session** 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
```

The following is sample output from the **show monitor session all** 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
```

The following is sample output from the **show monitor session erspan-source** command:

```
Switch# show monitor session erspan-source

Type : ERSPAN Source Session
Status : Admin Enabled
Source Ports :
RX Only : Gi1/4/33
Destination IP Address : 20.20.163.20
Destination ERSPAN ID : 110
Origin IP Address : 10.10.10.216
IPv6 Flow Label : None
```

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 Everest 16.5.1a	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 Denali 16.1.1	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-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** | **cluster** | **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** | **cluster** | **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.*
cluster	(Optional) Enables SNMP cluster 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 3.2SE	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 cluster
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 3.2SE	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 3.2SE	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 3.2SE	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 3.2SE	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 3.2SE	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 [**fan**] [**shutdown**] [**status**] [**supply**] [**temperature**]
no snmp-server enable traps envmon [**fan**] [**shutdown**] [**status**] [**supply**] [**temperature**]

Syntax Description

fan	(Optional) Enables fan traps.
shutdown	(Optional) Enables environmental monitor shutdown traps.
status	(Optional) Enables SNMP environmental status-change traps.
supply	(Optional) Enables environmental monitor power-supply traps.
temperature	(Optional) Enables environmental monitor temperature traps.

Command Default

The sending of environmental SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	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 fan traps:

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

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 3.2SE	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 3.2SE	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 3.2SE	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 3.2SE	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 3.2SE	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 3.2SE	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 3.2SE	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 3.2SE	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 3.2SE	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 3.2SE	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 stackwise

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

snmp-server enable traps stackwise [**GLS**] [**ILS**] [**SRLS**]
[**insufficient-power**] [**invalid-input-current**]
[**invalid-output-current**] [**member-removed**] [**member-upgrade-notification**]
[**new-master**] [**new-member**] [**port-change**] [**power-budget-warning**] [**power-invalid-topology**]
[**power-link-status-changed**] [**power-oper-status-changed**]
[**power-priority-conflict**] [**power-version-mismatch**] [**ring-redundant**]
[**stack-mismatch**] [**unbalanced-power-supplies**] [**under-budget**] [**under-voltage**]
no snmp-server enable traps stackwise [**GLS**] [**ILS**] [**SRLS**]
[**insufficient-power**] [**invalid-input-current**]
[**invalid-output-current**] [**member-removed**] [**member-upgrade-notification**]
[**new-master**] [**new-member**] [**port-change**] [**power-budget-warning**] [**power-invalid-topology**]
[**power-link-status-changed**] [**power-oper-status-changed**]
[**power-priority-conflict**] [**power-version-mismatch**] [**ring-redundant**]
[**stack-mismatch**] [**unbalanced-power-supplies**] [**under-budget**] [**under-voltage**]

Syntax Description

GLS	(Optional) Enables StackWise stack power GLS trap.
ILS	(Optional) Enables StackWise stack power ILS trap.
SRLS	(Optional) Enables StackWise stack power SRLS trap.
insufficient-power	(Optional) Enables StackWise stack power unbalanced power supplies trap.
invalid-input-current	(Optional) Enables StackWise stack power invalid input current trap.
invalid-output-current	(Optional) Enables StackWise stack power invalid output current trap.
member-removed	(Optional) Enables StackWise stack member removed trap.
member-upgrade-notification	(Optional) Enables StackWise member to be reloaded for upgrade trap.
new-master	(Optional) Enables StackWise new master trap.
new-member	(Optional) Enables StackWise stack new member trap.
port-change	(Optional) Enables StackWise stack port change trap.
power-budget-warning	(Optional) Enables StackWise stack power budget warning trap.
power-invalid-topology	(Optional) Enables StackWise stack power invalid topology trap.
power-link-status-changed	(Optional) Enables StackWise stack power link status changed trap.
power-oper-status-changed	(Optional) Enables StackWise stack power port oper status changed trap.
power-priority-conflict	(Optional) Enables StackWise stack power priority conflict trap.

power-version-mismatch	(Optional) Enables StackWise stack power version mismatch discovered trap.
ring-redundant	(Optional) Enables StackWise stack ring redundant trap.
stack-mismatch	(Optional) Enables StackWise stack mismatch trap.
unbalanced-power-supplies	(Optional) Enables StackWise stack power unbalanced power supplies trap.
under-budget	(Optional) Enables StackWise stack power under budget trap.
under-voltage	(Optional) Enables StackWise stack power under voltage trap.

Command Default

The sending of SNMP StackWise traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	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 StackWise stack power GLS traps:

```
Device(config)# snmp-server enable traps stackwise GLS
```

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.

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	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 3.2SE	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 3.2SE	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 3.2SE	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 3.2SE	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 Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	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 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. • **eigrp**—Sends SNMP EIGRP 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. • **isis**—Sends IS-IS traps. • **license**—Sends license traps. • **local-auth**—Sends SNMP local auth traps. • **mac-notification**—Sends SNMP MAC notification traps. • **ospf**—Sends Open Shortest Path First (OSPF) traps. • **pim**—Sends SNMP Protocol-Independent Multicast (PIM) traps. • **port-security**—Sends SNMP port-security 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. • **vstack**—Sends SNMP Smart Install traps. • **vtp**—Sends SNMP VLAN Trunking Protocol (VTP) 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 3.2SE	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.

source (ERSPAN)

To configure the Encapsulated Remote Switched Port Analyzer (ERSPAN) source interface or VLAN, and the traffic direction to be monitored, use the **source** command in ERSPAN monitor source session configuration mode. To disable the configuration, use the **no** form of this command.

source {**interface** *type number* | **vlan** *vlan-ID*}[{**,** | **-** | **both** | **rx** | **tx**}]

Syntax Description

interface *type number*	Specifies an interface type and number.
vlan *vlan-ID*	Associates the ERSPAN source session number with VLANs. Valid values are from 1 to 4094.
,	(Optional) Specifies another interface.
-	(Optional) Specifies a range of interfaces.
both	(Optional) Monitors both received and transmitted ERSPAN traffic.
rx	(Optional) Monitors only received traffic.
tx	(Optional) Monitors only transmitted traffic.

Command Default

Source interface or VLAN is not configured.

Command Modes

ERSPAN monitor source session configuration mode (config-mon-erspan-src)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

You cannot include source VLANs and filter VLANs in the same session.

Examples

The following example shows how to configure ERSPAN source session properties:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# source interface fastethernet 0/1 rx
```

Related Commands

Command	Description
monitor session type erspan-source	Configures a local ERSPAN source session.

status syslog

To send the status of provisioning policies to the syslog, use the **status syslog** command in auto-depoly configuration mode. To disable the configuration, use the **no** form of this command.

status syslog
no status syslog

This command has no arguments or keywords.

Command Default

Sylog debugging is not enabled.

Command Modes

Auto-deploy configuration (config-auto-deploy)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

Example

The following example shows how to enable syslog debugging:

```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# status syslog
```

Related Commands

Command	Description
event-manager auto-deploy	Configures an EEM auto-deployment profile.

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 3.3SE	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 3.3SE	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
```

window

To set a random time for profile provisioning to be triggered, use the **window** command in auto-deploy configuration mode. To remove the configuration, use the **no** form of this command.

window *minutes*
no window *minutes*

Syntax Description

minutes	Time in minutes. Valid values are from 1 to 60.

Command Default

Policy provisioning window is not enabled.

Command Modes

Auto-deploy configuration (config-auto-deploy)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

The window duration is added to the time configured by the **schedule start-in** command. Profile provisioning is triggered at random time between the specified schedule and the configured window duration.

Example

The following example shows how to set a random time for policy provisioning. In this example, the scheduled start time for policy provisioning is 2 hours and 30 minutes. When the window duration of 10 minutes is configured, this time is added to 2 hours and 30 minutes. Policy provisioning will start any time after 2 hour and 30 minutes; but within the 10 minutes specified as the window duration.

```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# schedule start-in hours 2 minutes 30 oneshot
Device(config-auto-deploy)# window 10
```

Related Commands

Command	Description
event-manager auto-deploy	Configures an EEM auto-deployment profile.