



Network Management Commands

- [active-timeout](#), on page 5
- [cache](#), on page 6
- [clear flow exporter](#), on page 8
- [clear flow monitor](#), on page 9
- [clear platform software fed switch swc connection](#), on page 11
- [clear platform software fed switch swc statistics](#), on page 12
- [clear snmp stats hosts](#), on page 13
- [collect](#), on page 14
- [collect counter](#), on page 15
- [collect flow sampler](#), on page 16
- [collect interface](#), on page 17
- [collect ipv4 destination](#), on page 18
- [collect ipv6 destination](#), on page 19
- [collect routing destination](#) , on page 20
- [collect ipv4 source](#), on page 21
- [collect ipv6 source](#), on page 23
- [collect routing source](#) , on page 25
- [collect timestamp absolute](#), on page 26
- [collect timestamp sys-uptime](#), on page 27
- [collect transport tcp flags](#), on page 29
- [collect routing next-hop address](#), on page 30
- [datalink flow monitor](#), on page 31
- [debug flow exporter](#), on page 32
- [debug flow monitor](#), on page 33
- [debug flow record](#), on page 34
- [debug sampler](#), on page 35
- [description](#), on page 36
- [description \(ERSPAN\)](#), on page 37
- [destination \(ERSPAN\)](#), on page 38
- [destination](#), on page 43
- [dscp](#), on page 44
- [et-analytics](#), on page 45
- [et-analytics enable](#), on page 46

- event manager applet, on page 47
- export-protocol netflow-v9, on page 50
- export-protocol netflow-v5, on page 51
- exporter, on page 52
- fconfigure, on page 53
- filter (ERSPAN), on page 54
- flow exporter, on page 56
- flow monitor, on page 57
- flow record, on page 58
- header-type, on page 59
- inactive time, on page 60
- ip flow-export destination, on page 61
- ip wccp, on page 62
- ip flow monitor, on page 64
- ipv6 flow monitor, on page 66
- ipv6 deny echo reply, on page 68
- match datalink ethertype, on page 69
- match datalink mac, on page 70
- match datalink vlan, on page 71
- match device-type, on page 72
- match flow cts, on page 73
- match flow direction, on page 74
- match interface, on page 75
- match ipv4, on page 76
- match ipv4 destination address, on page 77
- match ipv4 source address, on page 78
- match ipv4 ttl, on page 79
- match ipv6, on page 80
- match ipv6 destination address, on page 81
- match ipv6 hop-limit, on page 82
- match ipv6 source address, on page 83
- map platform-type, on page 84
- match transport, on page 85
- match transport icmp ipv4, on page 86
- match transport icmp ipv6, on page 87
- match platform-type, on page 88
- mode random 1 out-of, on page 89
- monitor capture (interface/control plane), on page 90
- monitor capture buffer, on page 92
- monitor capture clear, on page 93
- monitor capture export, on page 94
- monitor capture file, on page 95
- monitor capture limit, on page 97
- monitor capture match, on page 98
- monitor capture pktlen-range , on page 99
- monitor capture start, on page 100

- [monitor capture stop](#), on page 101
- [monitor session](#), on page 102
- [monitor session destination](#), on page 104
- [monitor session filter](#), on page 108
- [monitor session source](#), on page 110
- [monitor session type](#), on page 112
- [option](#), on page 114
- [pae](#), on page 116
- [record](#), on page 117
- [sensor-name \(stealthwatch-cloud-monitor\)](#), on page 118
- [service-key \(stealthwatch-cloud-monitor\)](#), on page 119
- [show flow monitor etta-mon cache](#), on page 120
- [sampler](#), on page 121
- [show capability feature monitor](#), on page 122
- [show class-map type control subscriber](#), on page 123
- [show flow exporter](#), on page 124
- [show flow interface](#), on page 126
- [show flow monitor](#), on page 128
- [show flow record](#), on page 130
- [show ip sla statistics](#), on page 131
- [show monitor](#), on page 133
- [show monitor capture](#), on page 135
- [show monitor session](#), on page 137
- [show parameter-map type subscriber attribute-to-service](#), on page 139
- [show platform software et-analytics](#), on page 140
- [show platform software fed switch active fnf et-analytics-flow-dump](#), on page 141
- [show platform software fed switch ip wccp](#), on page 142
- [show platform software fed switch swc connection](#), on page 144
- [show platform software fed switch swc statistics](#), on page 146
- [show platform software swspan](#), on page 148
- [show product-analytics kpi](#), on page 150
- [show product-analytics report](#), on page 152
- [show product-analytics stats](#), on page 154
- [show sampler](#), on page 156
- [show snmp stats](#), on page 158
- [show stealth-watch-cloud detail](#), on page 160
- [shutdown \(monitor session\)](#), on page 161
- [snmp ifmib ifindex persist](#), on page 162
- [snmp-server community](#), on page 163
- [snmp-server enable traps](#), on page 165
- [snmp-server enable traps bridge](#), on page 168
- [snmp-server enable traps bulkstat](#), on page 169
- [snmp-server enable traps call-home](#), on page 170
- [snmp-server enable traps cef](#), on page 171
- [snmp-server enable traps cpu](#), on page 172
- [snmp-server enable traps envmon](#), on page 173

- [snmp-server enable traps errdisable](#), on page 174
- [snmp-server enable traps flash](#), on page 175
- [snmp-server enable traps isis](#), on page 176
- [snmp-server enable traps mac-notification](#), on page 177
- [snmp-server enable traps ospf](#), on page 178
- [snmp-server enable traps pim](#), on page 179
- [snmp-server enable traps port-security](#), on page 180
- [snmp-server enable traps power-ethernet](#), on page 181
- [snmp-server enable traps snmp](#), on page 182
- [snmp-server enable traps stackwise](#), on page 183
- [snmp-server enable traps storm-control](#), on page 185
- [snmp-server enable traps stpx](#), on page 186
- [snmp-server enable traps transceiver](#), on page 187
- [snmp-server enable traps vrfmib](#), on page 188
- [snmp-server enable traps vstack](#), on page 189
- [snmp-server engineID](#), on page 190
- [snmp-server group](#), on page 191
- [snmp-server host](#), on page 195
- [snmp-server manager](#), on page 200
- [snmp-server user](#), on page 201
- [snmp-server view](#), on page 205
- [source](#), on page 207
- [source \(ERSPAN\)](#), on page 209
- [socket](#), on page 210
- [stealthwatch-cloud-monitor](#), on page 211
- [switchport mode access](#), on page 212
- [switchport voice vlan](#), on page 213
- [ttl](#), on page 214
- [transport](#), on page 215
- [template data timeout](#), on page 216
- [udp peek](#), on page 217
- [url \(stealthwatch-cloud-monitor\)](#), on page 218

active-timeout

To configure et-analytics active timer value, use the **active-timeout** *seconds* command in the et-analytics configuration mode.

To reset the timer settings to the default, use the **no** form of the command.

active-timeout *seconds*
no active-timeout *seconds*

| Syntax Description | active-timeout | Configures the active-timeout value. |
|--------------------|----------------|---|
| | <i>seconds</i> | Sets the active-timeout value in seconds. The supported range is from 1 to 604800, and the default value is 30 minutes. |

Command Modes et-analytics configuration (config-et-analytics)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.x | This command was introduced. |

Usage Guidelines Prior to the Cisco IOS XE Bengaluru 17.6.x release, the active-timeout value was set to 1800 seconds, by default. However, starting from Cisco IOS XE Bengaluru 17.6.x, you can configure the active-timeout value.

Example:

The following example shows how to configure an active-timeout of 300 seconds:

```
Device>enable
Device#configure terminal
Device(config)# et-analytics
Device(config-et-analytics)# active-timeout 300
```

cache

To configure a flow cache parameter for a flow monitor, use the **cache** command in flow monitor configuration mode. To remove a flow cache parameter for a flow monitor, use the **no** form of this command.

```
cache {timeout {active | inactive | rate-limit | update} seconds | type normal}
no cache {timeout {active | inactive | rate-limit | update} | type}
```

| Syntax Description | | |
|--------------------|--|---|
| timeout | | Specifies the flow timeout. |
| active | | Specifies the active flow timeout. |
| inactive | | Specifies the inactive flow timeout. |
| update | | Specifies the update timeout for a permanent flow cache. |
| <i>seconds</i> | | The timeout value in seconds. The range is 30 to 604800 (7 days) for a normal flow cache. For a permanent flow cache the range is 1 to 604800 (7 days). |
| type | | Specifies the type of the flow cache. |
| normal | | Configures a normal cache type. The entries in the flow cache will be aged out according to the timeout active seconds and timeout inactive seconds settings. This is the default cache type. |

Command Default

The default flow monitor flow cache parameters are used.

The following flow cache parameters for a flow monitor are enabled:

- Cache type: normal
- Active flow timeout: 1800 seconds

Command Modes

Flow monitor configuration

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

Each flow monitor has a cache that it uses to store all the flows it monitors. Each cache has various configurable elements, such as the time that a flow is allowed to remain in it. When a flow times out, it is removed from the cache and sent to any exporters that are configured for the corresponding flow monitor.

The **cache timeout active** command controls the aging behavior of the normal type of cache. If a flow has been active for a long time, it is usually desirable to age it out (starting a new flow for any subsequent packets in the flow). This age out process allows the monitoring application that is receiving the exports to remain up to date. By default, this timeout is 1800 seconds (30 minutes), but it can be adjusted according to system requirements. A larger value ensures that long-lived flows are accounted for in a single flow record; a smaller value results in a shorter delay between starting a new long-lived flow and exporting some data for it. When you change the active flow timeout, the new timeout value takes effect immediately.

The **cache timeout inactive** command also controls the aging behavior of the normal type of cache. If a flow has not seen any activity for a specified amount of time, that flow will be aged out. By default, this timeout is 15 seconds, but this value can be adjusted depending on the type of traffic expected. If a large number of short-lived flows is consuming many cache entries, reducing the inactive timeout can reduce this overhead. If a large number of flows frequently get aged out before they have finished collecting their data, increasing this timeout can result in better flow correlation. When you change the inactive flow timeout, the new timeout value takes effect immediately.

The **cache timeout update** command controls the periodic updates sent by the permanent type of cache. This behavior is similar to the active timeout, except that it does not result in the removal of the cache entry from the cache. By default, this timer value is 1800 seconds (30 minutes).

The **cache type normal** command specifies the normal cache type. This is the default cache type. The entries in the cache will be aged out according to the **timeout active** *seconds* and **timeout inactive** *seconds* settings. When a cache entry is aged out, it is removed from the cache and exported via any exporters configured for the monitor associated with the cache.

To return a cache to its default settings, use the **default cache** flow monitor configuration command.



Note When a cache becomes full, new flows will not be monitored.

The following example shows how to configure the active timeout for the flow monitor cache:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache timeout active 4800
```

The following example shows how to configure the inactive timer for the flow monitor cache:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache timeout inactive 30
```

The following example shows how to configure the permanent cache update timeout:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache timeout update 5000
```

The following example shows how to configure a normal cache:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache type normal
```

clear flow exporter

To clear the statistics for a Flexible Netflow flow exporter, use the **clear flow exporter** command in privileged EXEC mode.

clear flow exporter *[[name] exporter-name] statistics*

Syntax Description

| | |
|----------------------|--|
| name | (Optional) Specifies the name of a flow exporter. |
| <i>exporter-name</i> | (Optional) Name of a flow exporter that was previously configured. |
| statistics | Clears the flow exporter statistics. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

The **clear flow exporter** command removes all statistics from the flow exporter. These statistics will not be exported and the data gathered in the cache will be lost.

You can view the flow exporter statistics by using the **show flow exporter statistics** privileged EXEC command.

Examples

The following example clears the statistics for all of the flow exporters configured on the device:

```
Device# clear flow exporter statistics
```

The following example clears the statistics for the flow exporter named FLOW-EXPORTER-1:

```
Device# clear flow exporter FLOW-EXPORTER-1 statistics
```


clear flow monitor

To clear a flow monitor cache or flow monitor statistics and to force the export of the data in the flow monitor cache, use the **clear flow monitor** command in privileged EXEC mode.

```
clear flow monitor [name] monitor-name [{[cache] force-export | statistics}]
```

| Syntax Description | name | Specifies the name of a flow monitor. |
|--------------------|---------------------|--|
| | <i>monitor-name</i> | Name of a flow monitor that was previously configured. |
| | cache | (Optional) Clears the flow monitor cache information. |
| | force-export | (Optional) Forces the export of the flow monitor cache statistics. |
| | statistics | (Optional) Clears the flow monitor statistics. |

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines The **clear flow monitor cache** command removes all entries from the flow monitor cache. These entries will not be exported and the data gathered in the cache will be lost.



Note The statistics for the cleared cache entries are maintained.

The **clear flow monitor force-export** command removes all entries from the flow monitor cache and exports them using all flow exporters assigned to the flow monitor. This action can result in a short-term increase in CPU usage. Use this command with caution.

The **clear flow monitor statistics** command clears the statistics for this flow monitor.



Note The current entries statistic will not be cleared by the **clear flow monitor statistics** command because this is an indicator of how many entries are in the cache and the cache is not cleared with this command.

You can view the flow monitor statistics by using the **show flow monitor statistics** privileged EXEC command.

Examples

The following example clears the statistics and cache entries for the flow monitor named FLOW-MONITOR-1:

```
Device# clear flow monitor name FLOW-MONITOR-1
```

The following example clears the statistics and cache entries for the flow monitor named FLOW-MONITOR-1 and forces an export:

```
Device# clear flow monitor name FLOW-MONITOR-1 force-export
```

The following example clears the cache for the flow monitor named FLOW-MONITOR-1 and forces an export:

```
Device# clear flow monitor name FLOW-MONITOR-1 cache force-export
```

The following example clears the statistics for the flow monitor named FLOW-MONITOR-1:

```
Device# clear flow monitor name FLOW-MONITOR-1 statistics
```

clear platform software fed switch swc connection

To clear the connection details and events of the Stealthwatch Cloud integration, use the **clear platform software fed switch *switch-number* swc connection** command in privileged EXEC mode.

clear platform software fed switch { *switch-number* | **active** } **swc connection**

Syntax Description

switch { *switch-number* | **active** } Device for which you want to clear information.

- *switch_num*: Switch ID.
- **active**: Clears information for the active switch.

swc connection Clears the connection details and events.

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|-------------------------------|------------------------------|
| Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |

Examples

The following is a sample output of the **clear platform software fed switch active swc connection** command:

```
Device> enable
Device# clear platform software fed switch active swc connection
```

Related Commands

| Command | Description |
|--|---|
| clear platform software fed switch { <i>switch-number</i> active } swc statistics | Clears the statistical information of the Stealthwatch Cloud integration. |
| show platform software fed switch { <i>switch-number</i> active } swc connection | Displays the connection details and events of the Stealthwatch Cloud integration. |
| show stealth-watch-cloud detail | Displays the Stealthwatch Cloud registration status and its configured values. |
| stealthwatch-cloud-monitor | Configures the Stealthwatch Cloud monitor. |

clear platform software fed switch swc statistics

To clear the statistical information of the Stealthwatch Cloud integration, use the **clear platform software fed switch *switch-number* swc statistics** command in privileged EXEC mode.

clear platform software fed switch { *switch-number* | **active** } **swc statistics**

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|-------------------------------|------------------------------|
| Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |

Examples

The following is a sample output of the **clear platform software fed switch active swc statistics** command:

```
Device> enable
Device# clear platform software fed switch active swc statistics
```

Related Commands

| Command | Description |
|--|---|
| clear platform software fed switch { <i>switch-number</i> active } swc connection | Clears the connection details and events of the Stealthwatch Cloud integration. |
| show platform software fed switch { <i>switch-number</i> active } swc statistics | Displays the statistical information of the Stealthwatch Cloud integration. |
| show stealth-watch-cloud detail | Displays the Stealthwatch Cloud registration status and its configured values. |
| stealthwatch-cloud-monitor | Configures the Stealthwatch Cloud monitor. |

clear snmp stats hosts

To clear the NMS IP address, the number of times an NMS polls the agent, and the timestamp of polling, use the **clear snmp stats hosts** command in privileged EXEC mode.

clear snmp stats hosts

Syntax Description

This command has no arguments or keywords.

Command Default

The details of the SNMP managers polled to the SNMP agent is stored in the system.

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|-------------------------------|------------------------------|
| Cisco IOS XE Amsterdam 17.1.1 | This command was introduced. |

Usage Guidelines

Use the **clear snmp stats hosts** command to delete all the entries polled to the SNMP agent.

The following is sample output of the **clear snmp stats hosts** command.

```
Device# clear snmp stats hosts
Request Count          Last Timestamp          Address
```

collect

To configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record, use the **collect** command in flow record configuration mode.

collect {**counter** | **interface** | **timestamp** | **transport**}

Syntax Description

| | |
|------------------|--|
| counter | Configures the number of bytes or packets in a flow as a non-key field for a flow record. For more information, see <i>collect counter</i> . |
| interface | Configures the input and output interface name as a non-key field for a flow record. For more information, see <i>collect interface</i> . |
| timestamp | Configures the absolute time of the first seen or last seen packet in a flow as a non-key field for a flow record. For more information, see <i>collect timestamp absolute</i> . |
| transport | Enables the collecting of transport TCP flags from a flow record. For more information, see <i>collect transport tcp flags</i> . |

Command Default

Non-key fields are not configured for the flow monitor record.

Command Modes

Flow record configuration

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

The **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases the values for non-key fields are taken from only the first packet in the flow.



Note Although it is visible in the command-line help string, the **flow username** keyword is not supported.

The following example configures the total number of bytes in the flows as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter bytes long
```

collect counter

To configure the number of bytes or packets in a flow as a non-key field for a flow record, use the **collect counter** command in flow record configuration mode. To disable the use of the number of bytes or packets in a flow (counters) as a non-key field for a flow record, use the **no** form of this command.

Command Default

The number of bytes or packets in a flow is not configured as a non-key field.

Command Modes

Flow record configuration

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

To return this command to its default settings, use the **no collect counter** or **default collect counter** flow record configuration command.

The following example configures the total number of bytes in the flows as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#collect counter bytes long
```

The following example configures the total number of packets from the flows as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter packets long
```

collect flow sampler

To configure a flow sampler ID as a non-key field for the record, use the **collect flow sampler** command in flow record configuration mode. To disable the use of the flow sampler ID number as a non-key field for a flow record, use the **no** form of this command.

collect flow sampler

no collect flow sampler

Syntax Description This command has no arguments or keywords.

Command Default The flow sampler is not configured as non-key fields.

Command Modes Flow record configuration (config-flow-record)

| Release | Modification |
|-------------------------------|------------------------------|
| Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |

Usage Guidelines The **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases the values for non-key fields are taken from only the first packet in the flow.

The **collect flow sampler** command is useful when more than one flow sampler is being used with different sampling rates. The non-key field contains the ID of the flow sampler used to monitor the flow.

Examples

The following example shows how to configure the ID of the flow sampler that is assigned to the flow as a non-key field:

```
Device> enable
Device# configure terminal
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect flow sampler
```

Related Commands

| Command | Description |
|----------------------|---|
| flow exporter | Creates a flow exporter |
| flow record | Creates a flow record for Flexible NetFlow. |

collect interface

To configure the input interface name as a non-key field for a flow record, use the **collect interface** command in flow record configuration mode. To disable the use of the input interface as a non-key field for a flow record, use the **no** form of this command.

collect interface input
no collect interface input

| Syntax Description | input Configures the input interface name as a non-key field and enables collecting the input interface from the flows. | | | | |
|------------------------------|--|---------|--------------|------------------------------|------------------------------|
| Command Default | The input interface name is not configured as a non-key field. | | | | |
| Command Modes | Flow record configuration | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Everest 16.5.1a | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Everest 16.5.1a | This command was introduced. | | | | |

Usage Guidelines The Flexible NetFlow **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

To return this command to its default settings, use the **no collect interface** or **default collect interface** flow record configuration command.

The following example configures the input interface as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect interface input
```

collect ipv4 destination

To configure the IPv4 destination as a non-key field for a flow record, use the **collect ipv4 destination** command in flow record configuration mode. To disable the use of an IPv4 destination field as a non-key field for a flow record, use the **no** form of this command.

collect ipv4 destination {mask | prefix} [minimum-mask *mask*]

no collect ipv4 destination {mask | prefix} [minimum-mask *mask*]

Syntax Description

| | |
|---------------------------------|---|
| mask | Configures the IPv4 destination mask as a non-key field and enables collecting the value of the IPv4 destination mask from the flows. |
| prefix | Configures the prefix for the IPv4 destination as a non-key field and enables collecting the value of the IPv4 destination prefix from the flows. |
| minimum-mask <i>mask</i> | (Optional) Specifies the size, in bits, of the minimum mask. Range: 1 to 32. |

Command Default

The IPv4 destination is not configured as a non-key field.

Command Modes

Flow record configuration (config-flow-record)

Command History

| Release | Modification |
|-------------------------------|------------------------------|
| Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |

Usage Guidelines

The Flexible NetFlow **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases the values for non-key fields are taken from only the first packet in the flow.

Examples

The following example shows how to configure the IPv4 destination prefix from the flows that have a prefix of 16 bits as a non-key field:

```
Device> enable
Device> configure terminal
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect ipv4 destination prefix minimum-mask 16
```

Related Commands

| Command | Description |
|--------------------|---|
| flow record | Creates a flow record for Flexible NetFlow. |

collect ipv6 destination

To configure the IPv6 destination as a non-key field for a flow record, use the **collect ipv6 destination** command in flow record configuration mode. To disable the use of an IPv6 destination field as a non-key field for a flow record, use the **no** form of this command.

```
collect ipv6 destination { mask | prefix } [ minimum-mask mask ]
no collect ipv6 destination { mask | prefix } [ minimum-mask mask ]
```

| Syntax Description | mask | prefix | minimum-mask mask |
|--------------------|---|---|--|
| | Configures the IPv6 destination mask as a non-key field and enables collecting the value of the IPv6 destination mask from the flows. | Configures the prefix for the IPv6 destination as a non-key field and enables collecting the value of the IPv6 destination prefix from the flows. | (Optional) Specifies the size, in bits, of the minimum mask. Range: 1 to 32. |

Command Default The IPv6 destination is not configured as a non-key field.

Command Modes Flow record configuration (config-flow-record)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

Usage Guidelines The Flexible NetFlow **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases the values for non-key fields are taken from only the first packet in the flow.

Examples The following example shows how to configure the IPv6 destination prefix from the flows that have a prefix of 16 bits as a non-key field:

```
Device> enable
Device> configure terminal
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect ipv6 destination prefix minimum-mask 16
```

| Related Commands | Command | Description |
|------------------|--------------------|---|
| | flow record | Creates a flow record for Flexible NetFlow. |

collect routing destination

To configure one or more of the destination routing attribute fields as a nonkey field for a flow record, use the **collect routing destination** command in flow record configuration mode. This command also enables collecting the values from the flows. To disable using the destination routing attribute fields as a nonkey field for a flow record, use the **no** form of the command.

collect routing destination [as [4-octet | peer [[4-octet]]]]

| | |
|--------------------|---|
| destination | Configures one or more of the destination routing attributes fields as a nonkey field and enables collecting the values from the flows. |
| as | Configures the autonomous system field as a nonkey field and enables collecting the value in the autonomous system field from the flows. |
| 4-octet | (Optional) Configures the 32-bit autonomous system number as a nonkey field. |
| peer | (Optional) Configures the autonomous system number of the peer network as a nonkey field and enables collecting the value of the autonomous system number of the peer network from the flows. |

Command Default

The routing attributes are not configured as a nonkey field.

Command Modes

Flow record configuration (config-flow-record)

Command History

| Release | Modification |
|-----------------------------|------------------------------|
| Cisco IOS XE Dublin 17.12.1 | This command was introduced. |

Usage Guidelines

collect routing destination as [peer]

This command collects the 16-bit autonomous system number based on a lookup of the router's routing table using the destination IP address. The optional **peer** keyword provides the expected next network, as opposed to the destination network.

collect routing destination as 4-octet [peer 4-octet]

This command collects the 32-bit autonomous system number based on a lookup of the router's routing table using the destination IP address. The **peer** keyword provides the expected next network, as opposed to the destination network.

collect ipv4 source

To configure the IPv4 source as a non-key field for a flow record, use the **collect ipv4 source** command in flow record configuration mode. To disable the use of the IPv4 source field as a non-key field for a flow record, use the **no** form of this command.

```
collect ipv4 source {mask | prefix} [minimum-mask mask]
no collect ipv4 source {mask | prefix} [minimum-mask mask]
```

| Syntax Description | | |
|---------------------------------|--|---|
| mask | | Configures the mask for the IPv4 source as a non-key field and enables collecting the value of the IPv4 source mask from the flows. |
| prefix | | Configures the prefix for the IPv4 source as a non-key field and enables collecting the value of the IPv4 source prefix from the flows. |
| minimum-mask <i>mask</i> | | (Optional) Specifies the size, in bits, of the minimum mask. Range: 1 to 32. |

Command Default The IPv4 source is not configured as a non-key field.

Command Modes Flow record configuration (config-flow-record)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |

Usage Guidelines The **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases the values for non-key fields are taken from only the first packet in the flow.

collect ipv4 source prefix minimum-mask

The source prefix is the network part of an IPv4 source. The optional minimum mask allows more information to be gathered about large networks.

collect ipv4 source mask minimum-mask

The source mask is the number of bits that make up the network part of the source. The optional minimum mask allows a minimum value to be configured. This command is useful when there is a minimum mask configured for the source prefix field and the mask is to be used with the prefix. In this case, the values configured for the minimum mask should be the same for the prefix and mask fields.

Alternatively, if the collector is aware of the minimum mask configuration of the prefix field, the mask field can be configured without a minimum mask so that the true mask and prefix can be calculated.

Examples

The following example shows how to configure the IPv4 source prefix from flows that have a prefix of 16 bits as a non-key field:

```
Device> enable
Device# configure terminal
Device(config)# flow record FLOW-RECORD-1
```

collect ipv4 source

```
Device(config-flow-record)# collect ipv4 source prefix minimum-mask 16
```

Related Commands

| Command | Description |
|--------------------|---|
| flow record | Creates a flow record for Flexible NetFlow. |

collect ipv6 source

To configure the IPv6 source as a non-key field for a flow record, use the **collect ipv6 source** command in flow record configuration mode. To disable the use of the IPv6 source field as a non-key field for a flow record, use the **no** form of this command.

```
collect ipv6 source { mask | prefix } [ minimum-mask mask ]
no collect ipv6 source { mask | prefix } [ minimum-mask mask ]
```

Syntax Description

| | |
|--------------------------|---|
| mask | Configures the mask for the IPv6 source as a non-key field and enables collecting the value of the IPv6 source mask from the flows. |
| prefix | Configures the prefix for the IPv6 source as a non-key field and enables collecting the value of the IPv6 source prefix from the flows. |
| minimum-mask mask | (Optional) Specifies the size, in bits, of the minimum mask. Range: 1 to 32. |

Command Default

The IPv6 source is not configured as a non-key field.

Command Modes

Flow record configuration (config-flow-record)

| Release | Modification |
|-------------------------------|------------------------------|
| Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

Usage Guidelines

The **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases the values for non-key fields are taken from only the first packet in the flow.

collect ipv6 source prefix minimum-mask

The source prefix is the network part of an IPv6 source. The optional minimum mask allows more information to be gathered about large networks.

collect ipv6 source mask minimum-mask

The source mask is the number of bits that make up the network part of the source. The optional minimum mask allows a minimum value to be configured. This command is useful when there is a minimum mask configured for the source prefix field and the mask is to be used with the prefix. In this case, the values configured for the minimum mask should be the same for the prefix and mask fields.

Alternatively, if the collector is aware of the minimum mask configuration of the prefix field, the mask field can be configured without a minimum mask so that the true mask and prefix can be calculated.

Examples

The following example shows how to configure the IPv6 source prefix from flows that have a prefix of 16 bits as a non-key field:

```
Device> enable
Device# configure terminal
Device(config)# flow record FLOW-RECORD-1
```

```
Device(config-flow-record)# collect ipv6 source prefix minimum-mask 16
```


collect routing source

To configure one or more of the source routing attribute fields as a nonkey field for a flow record, use the **collect routing destination** command in flow record configuration mode. This command also enables collecting the values from the flows. To disable using the source routing attribute fields as a nonkey field for a flow record, use the **no** form of the command.

collect routing source [as [4-octet | peer [[4-octet]]]]

| | |
|----------------|---|
| source | Configures one or more of the source routing attributes fields as a nonkey field and enables collecting the values from the flows. |
| as | Configures the autonomous system field as a nonkey field and enables collecting the value in the autonomous system field from the flows. |
| 4-octet | (Optional) Configures the 32-bit autonomous system number as a nonkey field. |
| peer | (Optional) Configures the autonomous system number of the peer network as a nonkey field and enables collecting the value of the autonomous system number of the peer network from the flows. |

Command Default

The routing attributes are not configured as a nonkey field.

Command Modes

Flow record configuration (config-flow-record)

Command History

| Release | Modification |
|-----------------------------|------------------------------|
| Cisco IOS XE Dublin 17.12.1 | This command was introduced. |

Usage Guidelines

collect routing source as [peer]

This command collects the 16-bit autonomous system number based on a lookup of the router's routing table using the source IP address. The optional **peer** keyword provides the expected next network, as opposed to the originating network.

collect routing source as 4-octet [peer 4-octet]

This command collects the 32-bit autonomous system number based on a lookup of the router's routing table using the source IP address. The optional **peer** keyword provides the expected next network, as opposed to the originating network.

collect timestamp absolute

To configure the absolute time of the first seen or last seen packet in a flow as a non-key field for a flow record, use the **collect timestamp absolute** command in flow record configuration mode. To disable the use of the first seen or last seen packet in a flow as a non-key field for a flow record, use the **no** form of this command.

```
collect timestamp absolute {first | last}
no collect timestamp absolute {first | last}
```

| Syntax Description | |
|--------------------|---|
| first | Configures the absolute time of the first seen packet in a flow as a non-key field and enables collecting time stamps from the flows. |
| last | Configures the absolute time of the last seen packet in a flow as a non-key field and enables collecting time stamps from the flows. |

Command Default The absolute time field is not configured as a non-key field.

Command Modes Flow record configuration

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines The **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases the values for non-key fields are taken from only the first packet in the flow.

The following example configures time stamps based on the absolute time of the first seen packet in a flow as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect timestamp absolute first
```

The following example configures time stamps based on the absolute time of the last seen packet in a flow as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect timestamp absolute last
```

collect timestamp sys-uptime

To configure the system uptime of the first seen or last seen packet in a flow as a nonkey field for a flow record, use the **collect timestamp sys-uptime** command in flow record configuration mode. To disable the use of the first seen or last seen packet in a flow as a nonkey field for a flow record, use the **no** form of this command.

```
collect timestamp sys-uptime { first | last }
no collect timestamp sys-uptime { first | last }
```

Syntax Description

| | |
|--------------|--|
| first | Configures the system uptime for the time the first packet was seen from the flows as a nonkey field and enables collecting time stamps based on the system uptime for the time the first packet was seen from the flows. |
| last | Configures the system uptime for the time the last packet was seen from the flows as a nonkey field and enables collecting time stamps based on the system uptime for the time the most recent packet was seen from the flows. |

Command Default

The system uptime field is not configured as a nonkey field.

Command Modes

Flow record configuration (config-flow-record)

Command History

| Release | Modification |
|-----------------------------|------------------------------|
| Cisco IOS XE Dublin 17.12.1 | This command was introduced. |

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

Examples

The following example configures time stamps based on the system uptime for the time the first packet was seen from the flows as a nonkey field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect timestamp sys-uptime first
```

The following example configures the time stamps based on the system uptime for the time the most recent packet was seen from the flows as a nonkey field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect timestamp sys-uptime last
```

Related Commands

| Command | Description |
|---|---|
| flow record | Creates a flow record, and enters Flexible NetFlow flow record configuration mode. |
| flow record type performance-monitor | Creates a flow record, and enters Performance Monitor flow record configuration mode. |

collect transport tcp flags

To enable the collecting of transport TCP flags from a flow, use the **collect transport tcp flags** command in flow record configuration mode. To disable the collecting of transport TCP flags from the flow, use the **no** form of this command.

collect transport tcp flags
no collect transport tcp flags

| | | |
|---------------------------|---|------------------------------|
| Syntax Description | This command has no arguments or keywords. | |
| Command Default | The transport layer fields are not configured as a non-key field. | |
| Command Modes | Flow record configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines The values of the transport layer fields are taken from all packets in the flow. You cannot specify which TCP flag to collect. You can only specify to collect transport TCP flags. All TCP flags will be collected with this command. The following transport TCP flags are collected:

- **ack**—TCP acknowledgement flag
- **cwr**—TCP congestion window reduced flag
- **ece**—TCP ECN echo flag
- **fin**—TCP finish flag
- **psh**—TCP push flag
- **rst**—TCP reset flag
- **syn**—TCP synchronize flag
- **urg**—TCP urgent flag

To return this command to its default settings, use the **no collect collect transport tcp flags** or **default collect collect transport tcp flags** flow record configuration command.

The following example collects the TCP flags from a flow:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect transport tcp flags
```

collect routing next-hop address

To configure the next-hop address value as a non-key field and enable collecting information regarding the next hop from the flows, use the **collect routing next-hop address** command in flow record configuration mode. To disable the use of one or more of the routing attributes as a non-key field for a flow record, use the **no** form of this command.

```
collect routing next-hop address { ipv4 | ipv6 }
no collect routing next-hop address { ipv4 | ipv6 }
```

Syntax Description

| | |
|-------------|---|
| ipv4 | Specifies that the next-hop address value is an IPv4 address. |
| ipv6 | Specifies that the next-hop address value is an IPv6 address. |

Command Default

Next hop address value is not configured as a non-key field.

Command Modes

Flow record configuration (config-flow-record)

Command History

| Release | Modification |
|-------------------------------|---|
| Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |
| Cisco IOS XE Amsterdam 17.3.1 | The ipv6 keyword was introduced. |

Usage Guidelines

The **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases the values for non-key fields are taken from only the first packet in the flow.

Examples

The following example shows how to configure the next-hop address value as a non-key field:

```
Device> enable
Device# configure terminal
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect routing next-hop address ipv4
```

Related Commands

| Command | Description |
|--------------------|--|
| flow record | Creates a flow record, and enters Flexible NetFlow flow record configuration mode. |

datalink flow monitor

To apply a Flexible NetFlow flow monitor to an interface, use the **datalink flow monitor** command in interface configuration mode. To disable a Flexible NetFlow flow monitor, use the **no** form of this command.

```
datalink flow monitor monitor-name sampler sampler-name input
no datalink flow monitor monitor-name sampler sampler-name input
```

| Syntax Description | | |
|--------------------|------------------------------------|---|
| | <i>monitor-name</i> | Name of the flow monitor to apply to the interface. |
| | sampler <i>sampler-name</i> | Enables the specified flow sampler for the flow monitor. |
| | input | Monitors traffic that the switch receives on the interface. |

Command Default A flow monitor is not enabled.

Command Modes Interface configuration

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines Before you apply a flow monitor to an interface with the **datalink flow monitor** command, you must have already created the flow monitor using the **flow monitor** global configuration command and the flow sampler using the **sampler** global configuration command.

To enable a flow sampler for the flow monitor, you must have already created the sampler.



Note The **datalink flow monitor** command only monitors non-IPv4 and non-IPv6 traffic. To monitor IPv4 traffic, use the **ip flow monitor** command. To monitor IPv6 traffic, use the **ipv6 flow monitor** command.

This example shows how to enable Flexible NetFlow datalink monitoring on an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# datalink flow monitor FLOW-MONITOR-1 sampler FLOW-SAMPLER-1 input
```

debug flow exporter

To enable debugging output for Flexible Netflow flow exporters, use the **debug flow exporter** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug flow exporter [[name] exporter-name] [{error | event | packets number}]
no debug flow exporter [[name] exporter-name] [{error | event | packets number}]
```

Syntax Description

| | |
|----------------------|--|
| name | (Optional) Specifies the name of a flow exporter. |
| <i>exporter-name</i> | (Optional) The name of a flow exporter that was previously configured. |
| error | (Optional) Enables debugging for flow exporter errors. |
| event | (Optional) Enables debugging for flow exporter events. |
| packets | (Optional) Enables packet-level debugging for flow exporters. |
| <i>number</i> | (Optional) The number of packets to debug for packet-level debugging of flow exporters. The range is 1 to 65535. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Examples

The following example indicates that a flow exporter packet has been queued for process send:

```
Device# debug flow exporter
May 21 21:29:12.603: FLOW EXP: Packet queued for process send
```


debug flow monitor

To enable debugging output for Flexible NetFlow flow monitors, use the **debug flow monitor** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug flow monitor [{error | [name] monitor-name [{cache [error] | error | packets packets}]}]
no debug flow monitor [{error | [name] monitor-name [{cache [error] | error | packets packets}]}]
```

| Syntax Description | |
|---------------------|---|
| error | (Optional) Enables debugging for flow monitor errors for all flow monitors or for the specified flow monitor. |
| name | (Optional) Specifies the name of a flow monitor. |
| <i>monitor-name</i> | (Optional) Name of a flow monitor that was previously configured. |
| cache | (Optional) Enables debugging for the flow monitor cache. |
| cache error | (Optional) Enables debugging for flow monitor cache errors. |
| packets | (Optional) Enables packet-level debugging for flow monitors. |
| <i>packets</i> | (Optional) Number of packets to debug for packet-level debugging of flow monitors. The range is 1 to 65535. |

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Examples

The following example shows that the cache for FLOW-MONITOR-1 was deleted:

```
Device# debug flow monitor FLOW-MONITOR-1 cache
May 21 21:53:02.839: FLOW MON: 'FLOW-MONITOR-1' deleted cache
```

debug flow record

To enable debugging output for Flexible NetFlow flow records, use the **debug flow record** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug flow record [{{name} record-name | options {sampler-table} | [{{detailed | error}}]}]
no debug flow record [{{name} record-name | options {sampler-table} | [{{detailed | error}}]}]
```

Syntax Description

| | |
|----------------------|---|
| name | (Optional) Specifies the name of a flow record. |
| <i>record-name</i> | (Optional) Name of a user-defined flow record that was previously configured. |
| options | (Optional) Includes information on other flow record options. |
| sampler-table | (Optional) Includes information on the sampler tables. |
| detailed | (Optional) Displays detailed information. |
| error | (Optional) Displays errors only. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Examples

The following example enables debugging for the flow record:

```
Device# debug flow record FLOW-record-1
```

debug sampler

To enable debugging output for Flexible NetFlow samplers, use the **debug sampler** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug sampler [{detailed | error | [name] sampler-name [{detailed | error | sampling samples}]}]
no debug sampler [{detailed | error | [name] sampler-name [{detailed | error | sampling}]}]
```

| Syntax Description | Parameter | Description |
|--------------------|--------------------------------|---|
| | detailed | (Optional) Enables detailed debugging for sampler elements. |
| | error | (Optional) Enables debugging for sampler errors. |
| | name | (Optional) Specifies the name of a sampler. |
| | <i>sampler-name</i> | (Optional) Name of a sampler that was previously configured. |
| | sampling <i>samples</i> | (Optional) Enables debugging for sampling and specifies the number of samples to debug. |

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Examples

The following sample output shows that the debug process has obtained the ID for the sampler named SAMPLER-1:

```
Device# debug sampler detailed
*May 28 04:14:30.883: Sampler: Sampler(SAMPLER-1: flow monitor FLOW-MONITOR-1 (ip,Et1/0,0)
  get ID succeeded:1
*May 28 04:14:30.971: Sampler: Sampler(SAMPLER-1: flow monitor FLOW-MONITOR-1 (ip,Et0/0,I)
  get ID succeeded:1
```

description

To configure a description for a flow monitor, flow exporter, or flow record, use the **description** command in the appropriate configuration mode. To remove a description, use the **no** form of this command.

description *description*
no description *description*

Syntax Description

description Text string that describes the flow monitor, flow exporter, or flow record.

Command Default

The default description for a flow sampler, flow monitor, flow exporter, or flow record is "User defined."

Command Modes

The following command modes are supported:

Flow exporter configuration

Flow monitor configuration

Flow record configuration

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

To return this command to its default setting, use the **no description** or **default description** command in the appropriate configuration mode.

The following example configures a description for a flow monitor:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# description Monitors traffic to 172.16.0.1 255.255.0.0
```

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 Everest 16.5.1a | 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:

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

| Related Commands | Command | Description |
|------------------|-----------------------------|--|
| | monitor session type | Configures a local ERSPAN source or destination 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 Everest 16.5.1a | This command was introduced. |
| | Cisco IOS XE Amsterdam 17.1.1 | The ipv6 keyword was added in the source session destination configuration mode, for IPv6 ERSPAN support. |

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

After you enter **destination** command, the command mode changes from monitor source session configuration mode (config-mon-erspan-src) to source session destination configuration mode (config-mon-erspan-src-dst). In this mode, enter a question mark (?) at the system prompt to see the list of commands that are available:

| | |
|-----------------------------------|--|
| erspan-id <i>erspan-ID</i> | Configures the ID used by the destination session to identify the ERSPAN traffic. Valid values range from 1 to 1023. |
| exit | Exits monitor ERSPAN destination session source property mode. |

| | |
|---|---|
| <pre>ip { address <i>ipv4-address</i> dscp <i>dscp-value</i> ttl <i>ttl-value</i> }</pre> | <p>Specifies IP properties. You can configure the following options:</p> <ul style="list-style-type: none"> • address <i>ipv4-address</i>: Configures the IP address for the ERSPAN destination sessions. All ERSPAN source session (maximum 8) destination IP addresses need not be same. <p>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.</p> <ul style="list-style-type: none"> • dscp <i>dscp-value</i>: Configures the Differentiated Services Code Point (DSCP) values for packets in the ERSPAN traffic. Valid values are from 0 to 63. <p>To remove the dscp values, use the no form of this command.</p> <ul style="list-style-type: none"> • ttl <i>ttl-value</i>: Configures the Time to Live (TTL) values for packets in the ERSPAN traffic. Valid values are from 2 to 255. <p>To remove the TTL values, use the no form of this command.</p> |
| <pre>ipv6 { address <i>ipv6-address</i> dscp <i>dscp-value</i> flow-label ttl <i>ttl-value</i> }</pre> | <p>Specifies IPv6 properties. You can configure the following options:</p> <ul style="list-style-type: none"> • address <i>ipv6-address</i>: Configures the IPv6 address for the ERSPAN destination sessions. All ERSPAN source session (maximum 8) destination IPv6 address need not be same. <p>The ERSPAN source session destination IPv6 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.</p> <ul style="list-style-type: none"> • dscp <i>dscp-value</i>: Configures the Differentiated Services Code Point (DSCP) values for packets in the ERSPAN traffic. Valid values are from 0 to 63. <p>To remove the dscp values, use the no form of this command.</p> <ul style="list-style-type: none"> • flow-label: Configures the flow-label. Valid values are from 0 to 1048575. <ul style="list-style-type: none"> • ttl <i>ttl-value</i>: Configures the Time to Live (TTL) values for packets in the ERSPAN traffic. Valid values are from 2 to 255. <p>To remove the TTL values, use the no form of this command.</p> |
| <pre>mtu <i>bytes</i></pre> | <p>Specifies the maximum transmission unit (MTU) size for ERSPAN truncation. The default value is 9000 bytes.</p> |
| <pre>origin { ip address <i>ip-address</i> ipv6 address <i>ipv6-address</i> }</pre> | <p>Configures the source of the ERSPAN traffic. You can enter an IPv4 address or an IPv6 address.</p> |
| <pre>vrf <i>vrf-id</i></pre> | <p>Configures virtual routing and forwarding (VRF) in the destination session. Enter the VRF ID.</p> |

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

Examples

The following examples show how to configure an ERSPAN source session destination, enter the ERSPAN monitor destination session configuration mode, and configure the various properties.

The following example specifies the destination property **ip**:

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

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

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

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

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# ip dscp 15
```

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

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

The following example specifies the destination property **ipv6**:

```
Device(config)# monitor session 3 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)#ipv6 address 2001:DB8::1
Device(config-mon-erspan-src-dst)#
```

The following example shows how to configure DSCP value for ERSPAN traffic IPv6:

```
Device(config)# monitor session 3 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# ipv6 dscp 10
```

The following example shows how to configure flow-label value for ERSPAN traffic IPv6:

```
Device(config)# monitor session 3 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# ipv6 flow-label 6
```

The following example shows how to configure TTL value for ERSPAN traffic IPv6:


```
Device(config)# monitor session 3 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# ipv6 ttl 32
```

The following example shows how to specify an MTU of 1000 bytes:

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# mtu 1000
```

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 192.0.2.1
```

The following example shows how to configure an IPv6 address for an ERSPAN source session:

```
Switch(config)# monitor session 3 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# origin ipv6 address 2001:DB8:1::1
```

The following example shows how to configure VRF in the destination session:

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

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

```
Device# 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
-----
```

destination (ERSPAN)

```
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 |
|----------------------------|--|
| monitorsession type | Configures a local ERSPAN source or destination session. |

destination

To configure an export destination for a flow exporter, use the **destination** command in flow exporter configuration mode. To remove an export destination for a flow exporter, use the **no** form of this command.

destination {*hostnameip-address*}
no destination {*hostnameip-address*}

Syntax Description

hostname Hostname of the device to which you want to send the NetFlow information.

ip-address IPv4 address of the workstation to which you want to send the NetFlow information.

Command Default

An export destination is not configured.

Command Modes

Flow exporter configuration

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

Each flow exporter can have only one destination address or hostname.

When you configure a hostname instead of the IP address for the device, the hostname is resolved immediately and the IPv4 address is stored in the running configuration. If the hostname-to-IP-address mapping that was used for the original Domain Name System (DNS) name resolution changes dynamically on the DNS server, the device does not detect this, and the exported data continues to be sent to the original IP address, resulting in a loss of data.

To return this command to its default setting, use the **no destination** or **default destination** command in flow exporter configuration mode.

The following example shows how to configure the networking device to export the Flexible NetFlow cache entry to a destination system:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# destination 10.0.0.4
```

dscp

To configure a differentiated services code point (DSCP) value for flow exporter datagrams, use the **dscp** command in flow exporter configuration mode. To remove a DSCP value for flow exporter datagrams, use the **no** form of this command.

```
dscp dscp
no dscp dscp
```

| | |
|---------------------------|--|
| Syntax Description | <i>dscp</i> DSCP to be used in the DSCP field in exported datagrams. The range is 0 to 63. The default is 0. |
|---------------------------|--|

| | |
|------------------------|---|
| Command Default | The differentiated services code point (DSCP) value is 0. |
|------------------------|---|

| | |
|----------------------|-----------------------------|
| Command Modes | Flow exporter configuration |
|----------------------|-----------------------------|

| Command History | <table border="0" style="width: 100%;"> <tr> <th style="text-align: left;">Release</th> <th style="text-align: left;">Modification</th> </tr> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </table> | Release | Modification | Cisco IOS XE Everest 16.5.1a | This command was introduced. |
|------------------------------|---|---------|--------------|------------------------------|------------------------------|
| Release | Modification | | | | |
| Cisco IOS XE Everest 16.5.1a | This command was introduced. | | | | |

| | |
|-------------------------|---|
| Usage Guidelines | To return this command to its default setting, use the no dscp or default dscp flow exporter configuration command. |
|-------------------------|---|

The following example sets 22 as the value of the DSCP field in exported datagrams:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# dscp 22
```

et-analytics

To enter the global et-analytics configuration mode, use the **et-analytics** command in the global configuration mode.

et-analytics

| | | |
|---------------------------|-------------------------------|---|
| Syntax Description | et-analytics | Enter the global et-analytics configuration mode. |
| Command Default | Disabled. | |
| Command Modes | Global configuration (config) | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Example:

The following example shows how to enter the et-analytics configuration mode:

```
Device>enable
Device#configure terminal
Device(config)# et-analytics
```

et-analytics enable

To enable et-analytics configuration on a particular interface, use the **et-analytics enable** command in the interface configuration mode. To disable et-analytics, use the **no** form of the command.

et-analytics enable
no et-analytics enable

| | | |
|---------------------------|-------------------------------------|--|
| Syntax Description | et-analytics enable | Enables et-analytics on a particular interface.. |
| Command Default | Disabled. | |
| Command Modes | Interface configuration (config-if) | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Example:

The following example shows how to enable et-analytics on interface GigabitEthernet1/0/2.:

```
Device>enable
Device#configure terminal
Device(config)# interface gi1/0/2
Device(config-if)# et-analytics enable
```

event manager applet

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

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

| Syntax Description | |
|----------------------|--|
| <i>applet-name</i> | Name of the applet file. |
| authorization | (Optional) Specifies AAA authorization type for applet. |
| bypass | (Optional) Specifies EEM AAA authorization type bypass. |
| class | (Optional) Specifies the EEM policy class. |
| <i>class-options</i> | (Optional) The EEM policy class. You can specify either one of the following: <ul style="list-style-type: none"> • <i>class-letter</i>-- Letter from A to Z that identifies each policy class. You can specify any one <i>class-letter</i>. • default --Specifies the policies registered with the default class. |
| trap | (Optional) Generates a Simple Network Management Protocol (SNMP) trap when the policy is triggered. |

Command Default No EEM applets are registered.

Command Modes Global configuration (config)

Command History

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

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

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

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



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

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

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

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

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

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

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

The following is a sample AAA configuration.

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

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

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

Examples

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

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

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

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

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

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

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

Related Commands

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

export-protocol netflow-v9

To configure NetFlow Version 9 export as the export protocol for a Flexible NetFlow exporter, use the **export-protocol netflow-v9** command in flow exporter configuration mode.

export-protocol netflow-v9

Syntax Description This command has no arguments or keywords.

Command Default NetFlow Version 9 is enabled.

Command Modes Flow exporter configuration

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines The device does not support NetFlow v5 export format, only NetFlow v9 export format is supported.

The following example configures NetFlow Version 9 export as the export protocol for a NetFlow exporter:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# export-protocol netflow-v9
```

export-protocol netflow-v5

To configure NetFlow Version 5 export as the export protocol for a Flexible NetFlow exporter, use the **export-protocol netflow-v5** command in flow exporter configuration mode.

export-protocol netflow-v5

Syntax Description This command has no arguments or keywords.

Command Default NetFlow Version 5 is enabled.

Command Modes Flow exporter configuration

| Command History | Release | Modification |
|------------------------|---------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

exporter

To add a flow exporter for a flow monitor, use the **exporter** command in the appropriate configuration mode. To remove a flow exporter for a flow monitor, use the **no** form of this command.

exporter *exporter-name*
no exporter *exporter-name*

| | |
|---------------------------|--|
| Syntax Description | <i>exporter-name</i> Name of a flow exporter that was previously configured. |
|---------------------------|--|

| | |
|------------------------|--------------------------------|
| Command Default | An exporter is not configured. |
|------------------------|--------------------------------|

| | |
|----------------------|----------------------------|
| Command Modes | Flow monitor configuration |
|----------------------|----------------------------|

| Command History | Release | Modification |
|------------------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | You must have already created a flow exporter by using the flow exporter command before you can apply the flow exporter to a flow monitor with the exporter command. |
|-------------------------|--|

To return this command to its default settings, use the **no exporter** or **default exporter** flow monitor configuration command.

Examples

The following example configures an exporter for a flow monitor:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# exporter EXPORTER-1
```

fconfigure

To specify the options in a channel use the **fconfigure** command in the TCL configuration mode.

fconfigure *channel-name* **remote** [*host port*] **broadcast** *boolean* **vrf** *vrf-table-name*

| Syntax Description | remote | Configures a remote session. It supports both IPv4 and IPv6 addresses. |
|--------------------|-------------------------------|---|
| | broadcast | Enables or disables broadcasting. The value of the option must be a proper boolean value. |
| | vrf | Returns the local VRF table name for the specified socket. If no VRF Table has been configured for the given socket, TCL_ERROR will be returned and “No VRF table configured” will be appended to the interpreter result. |
| Command Default | TCL configuration mode | |
| Command Modes | TCL configuration mode | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.2.1 | The myvrf keyword was introduced. |

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

| Syntax Description | | |
|-----------------------------|--|---|
| ip | | Specifies the IP access control rules. |
| access-group | | Specifies an access control group. |
| <i>standard-access-list</i> | | Standard IP access list. |
| <i>extended-access-list</i> | | Extended IP access list. |
| <i>acl-name</i> | | Access list name. |
| ipv6 | | Specifies the IPv6 access control rules. |
| mac | | Specifies the media access control (MAC) rules. |
| sgt <i>sgt-ID</i> | | Specifies the Security Group Tag (SGT). Valid values are from 1 to 65535. |
| vlan <i>vlan-ID</i> | | 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 Everest 16.5.1a | This command was introduced. |
| | Cisco IOS XE Gibraltar 16.11.1 | The sgt keyword 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:

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

Related Commands

| Command | Description |
|-----------------------------|--|
| monitor session type | Configures a local ERSPAN source or destination session. |

flow exporter

To create a Flexible NetFlow flow exporter, or to modify an existing Flexible NetFlow flow exporter, and enter Flexible NetFlow flow exporter configuration mode, use the **flow exporter** command in global configuration mode. To remove a Flexible NetFlow flow exporter, use the **no** form of this command.

flow exporter *exporter-name*
no flow exporter *exporter-name*

| | |
|---------------------------|---|
| Syntax Description | <i>exporter-name</i> Name of the flow exporter that is being created or modified. |
|---------------------------|---|

| | |
|------------------------|---|
| Command Default | Flexible NetFlow flow exporters are not present in the configuration. |
|------------------------|---|

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

| Command History | Release | Modification |
|------------------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors. |
|-------------------------|---|

| | |
|-----------------|---|
| Examples | The following example creates a flow exporter named FLOW-EXPORTER-1 and enters Flexible NetFlow flow exporter configuration mode: |
|-----------------|---|

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)#
```


flow monitor

To create a flow monitor, or to modify an existing flow monitor, and enter flow monitor configuration mode, use the **flow monitor** command in global configuration mode. To remove a flow monitor, use the **no** form of this command.

flow monitor *monitor-name*
no flow monitor *monitor-name*

| | |
|---------------------------|---|
| Syntax Description | <i>monitor-name</i> Name of the flow monitor that is being created or modified. |
|---------------------------|---|

| | |
|------------------------|--|
| Command Default | Flexible NetFlow flow monitors are not present in the configuration. |
|------------------------|--|

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

| Command History | Release | Modification |
|------------------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | Flow monitors are the Flexible NetFlow component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a flow record and a cache. You add the record to the flow monitor after you create the flow monitor. The flow monitor cache is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in the flow monitor's record and stored in the flow monitor cache. |
|-------------------------|---|

| | |
|-----------------|---|
| Examples | The following example creates a flow monitor named FLOW-MONITOR-1 and enters flow monitor configuration mode: |
|-----------------|---|

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)#
```

flow record

To create a Flexible NetFlow flow record, or to modify an existing Flexible NetFlow flow record, and enter Flexible NetFlow flow record configuration mode, use the **flow record** command in global configuration mode. To remove a Flexible NetFlow record, use the **no** form of this command.

flow record *record-name*
no flow record *record-name*

| | |
|---------------------------|---|
| Syntax Description | <i>record-name</i> Name of the flow record that is being created or modified. |
|---------------------------|---|

| | |
|------------------------|---|
| Command Default | A Flexible NetFlow flow record is not configured. |
|------------------------|---|

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

| Command History | Release | Modification |
|------------------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | A flow record defines the keys that Flexible NetFlow uses to identify packets in the flow, as well as other fields of interest that Flexible NetFlow gathers for the flow. You can define a flow record with any combination of keys and fields of interest. The device supports a rich set of keys. A flow record also defines the types of counters gathered per flow. You can configure 64-bit packet or byte counters. |
|-------------------------|--|

Examples

The following example creates a flow record named FLOW-RECORD-1, and enters Flexible NetFlow flow record configuration mode:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#
```

header-type

To configure the ERSPAN header type for encapsulation, use the **header-type** command in ERSPAN monitor source session configuration mode. To remove the configuration, use the **no** form of this command.

```
header-type header-type
no header-type header-type
```

| | |
|---------------------------|--|
| Syntax Description | <i>header-type</i> ERSPAN header type. Valid header types are 2 and 3. |
|---------------------------|--|

| | |
|------------------------|---------------------------------|
| Command Default | ERSPAN header type is set to 2. |
|------------------------|---------------------------------|

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

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Examples

The following example shows how to change the ERSPAN header type to 3:

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# header-type 3
```

| Related Commands | Command | Description |
|-------------------------|-----------------------------|--|
| | monitor session type | Configures a local ERSPAN source or destination session. |

inactive time

To configure et-analytics inactive timer value, use the **inactive time *seconds*** command in the et-analytics configuration mode. To disable the timer settings, use the **no** form of the command.

inactive time *seconds*
no inactive time *seconds*

| | | |
|---------------------------|--|--|
| Syntax Description | inactive time | Configures the inactive timer value. |
| | <i>seconds</i> | Timer value in seconds. The range is from 1 to 604800 and the default value is 60 seconds. |
| Command Default | Disabled. | |
| Command Modes | et-analytics configuration (config-et-analytics) | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Example:

The following example shows how to configure an inactive timer of 10 seconds:

```
Device>enable
Device#configure terminal
Device(config)# et-analytics
Device(config-et-analytics)# inactive time 10
```

ip flow-export destination

To configure the global collector destination IP address, use the **ip flow-export destination** *ip_address port* command in the et-analytics configuration mode. To remove the collector destination IP address, use the **no** form of the command.

ip flow-export destination *ip_address port*
no ip flow-export destination *ip_address port*

| | | |
|---------------------------|--|--|
| Syntax Description | ip flow-export destination | Configures the global collector destination IP address and port. |
| | <i>ip_address</i> | Destination IP address. |
| | <i>port</i> | Destination port. |
| Command Default | Disabled. | |
| Command Modes | et-analytics configuration (config-et-analytics) | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Example:

The following example shows how to configure a flow-exporter destination IP address of 10.1.1.1 and port 2055:

```
Device>enable
Device#configure terminal
Device(config)# et-analytics
Device(config-et)# ip flow-export destination 10.1.1.1 2055
```

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). |
| <i>service-number</i> | | 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 <i>groupaddress</i> | | (Optional) Specifies the multicast group address used by the device and the application engines to participate in the service group. |
| group-list <i>access-list</i> | | (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 <i>access-list</i> | | (Optional) Specifies the redirect service for specific hosts or specific packets from hosts. |
| password <i>encryption-number</i> <i>password</i> | | (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 Everest 16.5.1a | 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
```

ip flow monitor

To enable a Flexible NetFlow flow monitor for IPv4 traffic that the device is receiving, use the **ip flow monitor** command in interface configuration mode. To disable a flow monitor, use the **no** form of this command.

```
ip flow monitor monitor-name [sampler sampler-name] input
no ip flow monitor monitor-name [sampler sampler-name] input
```

| Syntax Description | |
|------------------------------------|---|
| <i>monitor-name</i> | Name of the flow monitor to apply to the interface. |
| sampler <i>sampler-name</i> | (Optional) Enables the specified flow sampler for the flow monitor. |
| input | Monitors IPv4 traffic that the device receives on the interface. |

Command Default A flow monitor is not enabled.

Command Modes Interface configuration

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

Before you can apply a flow monitor to an interface with the **ip flow monitor** command, you must have already created the flow monitor using the **flow monitor** global configuration command.

When you add a sampler to a flow monitor, only packets that are selected by the named sampler will be entered into the cache to form flows. Each use of a sampler causes separate statistics to be stored for that usage.

You cannot add a sampler to a flow monitor after the flow monitor has been enabled on the interface. You must first remove the flow monitor from the interface and then enable the same flow monitor with a sampler.



Note The statistics for each flow must be scaled to give the expected true usage. For example, with a 1 in 100 sampler it is expected that the packet and byte counters will have to be multiplied by 100.

The following example enables a flow monitor for monitoring input traffic:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

The following example enables a flow monitor for monitoring input traffic, with a sampler to limit the input packets that are sampled:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

The following example shows what happens when you try to add a sampler to a flow monitor that has already been enabled on an interface without a sampler:


```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

The following example shows how to remove a flow monitor from an interface so that it can be enabled with the sampler:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

ipv6 flow monitor

To enable a flow monitor for IPv6 traffic that the device is receiving, use the **ipv6 flow monitor** command in interface configuration mode. To disable a flow monitor, use the **no** form of this command.

```
ipv6 flow monitor monitor-name [sampler sampler-name] input
no ipv6 flow monitor monitor-name [sampler sampler-name] input
```

| Syntax Description | | |
|--------------------|------------------------------------|---|
| | <i>monitor-name</i> | Name of the flow monitor to apply to the interface. |
| | sampler <i>sampler-name</i> | (Optional) Enables the specified flow sampler for the flow monitor. |
| | input | Monitors IPv6 traffic that the device receives on the interface. |

Command Default A flow monitor is not enabled.

Command Modes Interface configuration

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines Before you can apply a flow monitor to the interface with the **ipv6 flow monitor** command, you must have already created the flow monitor using the **flow monitor** global configuration command.

When you add a sampler to a flow monitor, only packets that are selected by the named sampler will be entered into the cache to form flows. Each use of a sampler causes separate statistics to be stored for that usage.

You cannot add a sampler to a flow monitor after the flow monitor has been enabled on the interface. You must first remove the flow monitor from the interface and then enable the same flow monitor with a sampler.



Note The statistics for each flow must be scaled to give the expected true usage. For example, with a 1 in 100 sampler it is expected that the packet and byte counters will have to be multiplied by 100.

The following example enables a flow monitor for monitoring input traffic:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
```

The following example enables a flow monitor for monitoring input traffic, with a sampler to limit the input packets that are sampled:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

The following example shows what happens when you try to add a sampler to a flow monitor that has already been enabled on an interface without a sampler:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

The following example shows how to remove a flow monitor from an interface so that it can be enabled with the sampler:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no ipv6 flow monitor FLOW-MONITOR-1 input
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

ipv6 deny echo reply

To disable the generation of ICMP IPv6 echo reply message to an IPv6 multicast address or anycast address, use the **ipv6 deny-echo-reply** command in the global configuration mode. To enable the generation of ICMP IPv6 echo reply message, use the **no** form of the command.

ipv6 deny-echo-reply
no ipv6 deny-echo-reply

Command Default ICMPv6 Echo Reply messages are sent from the device.

Command Modes Global configuration (config)

| Command History | Release | Modification |
|-----------------|-------------------------------|-----------------------------|
| | Cisco IOS XE Amsterdam 17.3.1 | The command was introduced. |

Usage Guidelines The **ipv6 deny-echo-reply** command works only for an IPv6 multicast or anycast address. It does not suppress an echo reply message for an IPv6 unicast address.

The following example shows how to configure a device to stop sending a response to an ICMPv6 echo message:

```
Device# configure terminal
Device(config)#ipv6 deny-echo-reply
Router(config)#end
```

The following example shows how to remove the **ipv6 deny-echo-reply** configuration:

```
Device# configure terminal
Device(config)#no ipv6 deny-echo-reply
Router(config)#end
```

match datalink ethertype

To configure the EtherType of the packet as a key field for a flow record, use the **match datalink ethertype** command in flow record configuration mode. To disable the EtherType of the packet as a key field for a flow record, use the **no** form of this command.

match datalink ethertype
no match datalink ethertype

Syntax Description This command has no arguments or keywords.

Command Default The EtherType of the packet is not configured as a key field.

Command Modes Flow record configuration

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

When you configure the EtherType of the packet as a key field for a flow record using the **match datalink ethertype** command, the traffic flow that is created is based on the type of flow monitor that is assigned to the interface:

- When a datalink flow monitor is assigned to an interface using the **datalink flow monitor** interface configuration command, it creates unique flows for different Layer 2 protocols.
- When an IP flow monitor is assigned to an interface using the **ip flow monitor** interface configuration command, it creates unique flows for different IPv4 protocols.
- When an IPv6 flow monitor is assigned to an interface using the **ipv6 flow monitor** interface configuration command, it creates unique flows for different IPv6 protocols.

To return this command to its default settings, use the **no match datalink ethertype** or **default match datalink ethertype** flow record configuration command.

The following example configures the EtherType of the packet as a key field for a Flexible NetFlow flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink ethertype
```

match datalink mac

To configure the use of MAC addresses as a key field for a flow record, use the **match datalink mac** command in flow record configuration mode. To disable the use of MAC addresses as a key field for a flow record, use the **no** form of this command.

```
match datalink mac {destination address input | source address input}
no match datalink mac {destination address input | source address input}
```

| Syntax Description | Field | Description |
|--------------------|--|---|
| | destination address | Configures the use of the destination MAC address as a key field. |
| | input | Specifies the MAC address of input packets. |
| | source address | Configures the use of the source MAC address as a key field. |
| Command Default | MAC addresses are not configured as a key field. | |
| Command Modes | Flow record configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The **input** keyword is used to specify the observation point that is used by the **match datalink mac** command to create flows based on the unique MAC addresses in the network traffic.



Note When a datalink flow monitor is assigned to an interface or VLAN record, it creates flows only for non-IPv6 or non-IPv4 traffic.

To return this command to its default settings, use the **no match datalink mac** or **default match datalink mac** flow record configuration command.

The following example configures the use of the destination MAC address of packets that are received by the device as a key field for a flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink mac destination address input
```

match datalink vlan

To configure the VLAN ID as a key field for a flow record, use the **match datalink vlan** command in flow record configuration mode. To disable the use of the VLAN ID value as a key field for a flow record, use the **no** form of this command.

```
match datalink vlan input
no match datalink vlan input
```

| Syntax Description | input Configures the VLAN ID of traffic being received by the device as a key field. | | | | |
|------------------------------|---|---------|--------------|------------------------------|------------------------------|
| Command Default | The VLAN ID is not configured as a key field. | | | | |
| Command Modes | Flow record configuration | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Everest 16.5.1a | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Everest 16.5.1a | This command was introduced. | | | | |
| Usage Guidelines | <p>A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the match command.</p> <p>The input keyword is used to specify the observation point that is used by the match datalink vlan command to create flows based on the unique VLAN IDs in the network traffic.</p> <p>The following example configures the VLAN ID of traffic being received by the device as a key field for a flow record:</p> <pre>Device(config)# flow record FLOW-RECORD-1 Device(config-flow-record)# match datalink vlan input</pre> | | | | |

match device-type

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

match device-type { *device-name* | **regex** *regular-expression* }

no match device-type

| | | |
|---------------------------|--|--|
| Syntax Description | <i>device-name</i> | Device name for the class map attribute filter criteria. |
| | regex <i>regular-expression</i> | Regular expression to specify the filter type. |

Command Default No default behavior or values.

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

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Examples

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

```
Device> enable
Device# configure terminal
Device(config)# class-map type control subscriber match-all DOT1X_NO_AGENT
Device(config-filter-control-classmap)# match device-type regex cis*
```


match flow cts

To configure CTS source group tag and destination group tag for a flow record, use the **match flow cts** command in flow record configuration mode. To disable the group tag as key field for a flow record, use the **no** form of this command.

```
match flow cts {source | destination} group-tag
no match flow cts {source | destination} group-tag
```

| | | |
|---------------------------|---|--|
| Syntax Description | cts destination group-tag | Configures the CTS destination field group as a key field. |
| | cts source group-tag | Configures the CTS source field group as a key field. |
| Command Default | The CTS destination or source field group, flow direction and the flow sampler ID are not configured as key fields. | |
| Command Modes | Flexible NetFlow flow record configuration (config-flow-record) Policy inline configuration (config-if-policy-inline) | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.5.1a | The command was introduced. |
| Usage Guidelines | <p>A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the match command.</p> <p>The following example configures the source group-tag as a key field:</p> <pre>Device(config)# flow record FLOW-RECORD-1 Device(config-flow-record)# match flow cts source group-tag</pre> | |

match flow direction

To configure the flow direction as key fields for a flow record, use the **match flow direction** command in flow record configuration mode. To disable the use of the flow direction as key fields for a flow record, use the **no** form of this command.

match flow direction
no match flow direction

Syntax Description This command has no arguments or keywords.

Command Default The flow direction is not configured as key fields.

Command Modes Flow record configuration

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The **match flow direction** command captures the direction of the flow as a key field. This feature is most useful when a single flow monitor is configured for input and output flows. It can be used to find and eliminate flows that are being monitored twice, once on input and once on output. This command can help to match up pairs of flows in the exported data when the two flows are flowing in opposite directions.

The following example configures the direction the flow was monitored in as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match flow direction
```

match interface

To configure the input and output interfaces as key fields for a flow record, use the **match interface** command in flow record configuration mode. To disable the use of the input and output interfaces as key fields for a flow record, use the **no** form of this command.

```
match interface {input | output}
no match interface {input | output}
```

Syntax Description

input Configures the input interface as a key field.

output Configures the output interface as a key field.

Command Default

The input and output interfaces are not configured as key fields.

Command Modes

Flow record configuration

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the input interface as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match interface input
```

The following example configures the output interface as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match interface output
```

match ipv4

To configure one or more of the IPv4 fields as a key field for a flow record, use the **match ipv4** command in flow record configuration mode. To disable the use of one or more of the IPv4 fields as a key field for a flow record, use the **no** form of this command.

match ipv4 {destination address | protocol | source address | tos | version}

no match ipv4 {destination address | protocol | source address | tos | version}

Syntax Description

| | |
|----------------------------|--|
| destination address | Configures the IPv4 destination address as a key field. For more information see <i>match ipv4 destination address</i> . |
| protocol | Configures the IPv4 protocol as a key field. |
| source address | Configures the IPv4 destination address as a key field. For more information see <i>match ipv4 source address</i> . |
| tos | Configures the IPv4 ToS as a key field. |
| version | Configures the IP version from IPv4 header as a key field. |

Command Default

The use of one or more of the IPv4 fields as a key field for a user-defined flow record is not enabled.

Command Modes

Flow record configuration

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the IPv4 protocol as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 protocol
```

match ipv4 destination address

To configure the IPv4 destination address as a key field for a flow record, use the **match ipv4 destination address** command in flow record configuration mode. To disable the IPv4 destination address as a key field for a flow record, use the **no** form of this command.

match ipv4 destination address
no match ipv4 destination address

Syntax Description

This command has no arguments or keywords.

Command Default

The IPv4 destination address is not configured as a key field.

Command Modes

Flow record configuration

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

To return this command to its default settings, use the **no match ipv4 destination address** or **default match ipv4 destination address** flow record configuration command.

The following example configures the IPv4 destination address as a key field for a flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 destination address
```

match ipv4 source address

To configure the IPv4 source address as a key field for a flow record, use the **match ipv4 source address** command in flow record configuration mode. To disable the use of the IPv4 source address as a key field for a flow record, use the **no** form of this command.

match ipv4 source address
no match ipv4 source address

Syntax Description This command has no arguments or keywords.

Command Default The IPv4 source address is not configured as a key field.

Command Modes Flow record configuration

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

To return this command to its default settings, use the **no match ipv4 source address** or **default match ipv4 source address** flow record configuration command.

The following example configures the IPv4 source address as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 source address
```

match ipv4 ttl

To configure the IPv4 time-to-live (TTL) field as a key field for a flow record, use the **match ipv4 ttl** command in flow record configuration mode. To disable the use of the IPv4 TTL field as a key field for a flow record, use the **no** form of this command.

match ipv4 ttl
no match ipv4 ttl

| Syntax Description | This command has no arguments or keywords. | | | | |
|------------------------------|--|---------|--------------|------------------------------|------------------------------|
| Command Default | The IPv4 time-to-live (TTL) field is not configured as a key field. | | | | |
| Command Modes | Flow record configuration | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Everest 16.5.1a</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Everest 16.5.1a | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Everest 16.5.1a | This command was introduced. | | | | |

Usage Guidelines A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match ipv4 ttl** command.

The following example configures IPv4 TTL as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 ttl
```

match ipv6

To configure one or more of the IPv6 fields as a key field for a flow record, use the **match ipv6** command in flow record configuration mode. To disable the use of one or more of the IPv6 fields as a key field for a flow record, use the **no** form of this command.

```
match ipv6 {destination address | protocol | source address | traffic-class | version}
no match ipv6 {destination address | protocol | source address | traffic-class | version}
```

| | | |
|---------------------------|--|--|
| Syntax Description | destination address | Configures the IPv4 destination address as a key field. For more information see <i>match ipv6 destination address</i> . |
| | protocol | Configures the IPv6 protocol as a key field. |
| | source address | Configures the IPv4 destination address as a key field. For more information see <i>match ipv6 source address</i> . |
| Command Default | The IPv6 fields are not configured as a key field. | |
| Command Modes | Flow record configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |
| Usage Guidelines | A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the match command. | |

The following example configures the IPv6 protocol field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 protocol
```


match ipv6 destination address

To configure the IPv6 destination address as a key field for a flow record, use the **match ipv6 destination address** command in flow record configuration mode. To disable the IPv6 destination address as a key field for a flow record, use the **no** form of this command.

```
match ipv6 destination address
no match ipv6 destination address
```

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no arguments or keywords. | |
| Command Default | The IPv6 destination address is not configured as a key field. | |
| Command Modes | Flow record configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

To return this command to its default settings, use the **no match ipv6 destination address** or **default match ipv6 destination address** flow record configuration command.

The following example configures the IPv6 destination address as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 destination address
```

match ipv6 hop-limit

To configure the IPv6 hop limit as a key field for a flow record, use the **match ipv6 hop-limit** command in flow record configuration mode. To disable the use of a section of an IPv6 packet as a key field for a flow record, use the **no** form of this command.

match ipv6 hop-limit
no match ipv6 hop-limit

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the IPv6 hop limit as a key field for a user-defined flow record is not enabled by default.

Command Modes

Flow record configuration

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the hop limit of the packets in the flow as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 hop-limit
```

match ipv6 source address

To configure the IPv6 source address as a key field for a flow record, use the **match ipv6 source address** command in flow record configuration mode. To disable the use of the IPv6 source address as a key field for a flow record, use the **no** form of this command.

match ipv6 source address
no match ipv6 source address

| Syntax Description | This command has no arguments or keywords. | | | | |
|------------------------------|--|---------|--------------|------------------------------|------------------------------|
| Command Default | The IPv6 source address is not configured as a key field. | | | | |
| Command Modes | Flow record configuration | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Everest 16.5.1a</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Everest 16.5.1a | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Everest 16.5.1a | This command was introduced. | | | | |

Usage Guidelines A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

To return this command to its default settings, use the **no match ipv6 source address** or **default match ipv6 source address** flow record configuration command.

The following example configures a IPv6 source address as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 source address
```

map platform-type

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

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

Syntax Description

| | |
|----------------------|---|
| <i>map-number</i> | Parameter map number. |
| eq | Specifies that the filter type name is equal to the platform type name. |
| not-eq | Specifies that the filter type name is not equal to the platform type name. |
| regex | Specifies that the filter type name is a regular expression. |
| <i>platform-type</i> | Platform type for the parameter map attribute filter criteria. |

Command Default

No default behavior or values.

Command Modes

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

Command History

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

Examples

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

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

Related Commands

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

match transport

To configure one or more of the transport fields as a key field for a flow record, use the **match transport** command in flow record configuration mode. To disable the use of one or more of the transport fields as a key field for a flow record, use the **no** form of this command.

Syntax Description

destination-port Configures the transport destination port as a key field.

source-port Configures the transport source port as a key field.

Command Default

The transport fields are not configured as a key field.

Command Modes

Flow record configuration

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the destination port as a key field:

```
(config)# flow record FLOW-RECORD-1
(config-flow-record)# match transport destination-port
```

The following example configures the source port as a key field:

```
(config)# flow record FLOW-RECORD-1
(config-flow-record)# match transport source-port
```

match transport icmp ipv4

To configure the ICMP IPv4 type field and the code field as key fields for a flow record, use the **match transport icmp ipv4** command in flow record configuration mode. To disable the use of the ICMP IPv4 type field and code field as key fields for a flow record, use the **no** form of this command.

```
match transport icmp ipv4 {code | type}
no match transport icmp ipv4 {code | type}
```

Syntax Description

code Configures the IPv4 ICMP code as a key field.

type Configures the IPv4 ICMP type as a key field.

Command Default

The ICMP IPv4 type field and the code field are not configured as key fields.

Command Modes

Flow record configuration

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the IPv4 ICMP code field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv4 code
```

The following example configures the IPv4 ICMP type field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv4 type
```

match transport icmp ipv6

To configure the ICMP IPv6 type field and the code field as key fields for a flow record, use the **match transport icmp ipv6** command in flow record configuration mode. To disable the use of the ICMP IPv6 type field and code field as key fields for a flow record, use the **no** form of this command.

```
match transport icmp ipv6 {code | type}
no match transport icmp ipv6 {code | type}
```

Syntax Description

code Configures the IPv6 ICMP code as a key field.

type Configures the IPv6 ICMP type as a key field.

Command Default

The ICMP IPv6 type field and the code field are not configured as key fields.

Command Modes

Flow record configuration

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the IPv6 ICMP code field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv6 code
```

The following example configures the IPv6 ICMP type field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv6 type
```

match platform-type

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

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

| | |
|---------------------------|--|
| Syntax Description | <i>platform-name</i> Name of the platform. |
|---------------------------|--|

| | |
|------------------------|--------------------------------|
| Command Default | No default behavior or values. |
|------------------------|--------------------------------|

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

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

Examples

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

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

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

mode random 1 out-of

To enable random sampling and to specify the packet interval for a Flexible NetFlow sampler, use the **mode random 1 out-of** command in sampler configuration mode. To remove the packet interval information for a Flexible NetFlow sampler, use the **no** form of this command.

```
mode random 1 out-of window-size
no mode
```

| | |
|---------------------------|--|
| Syntax Description | <i>window-size</i> Specifies the window size from which to select packets. The range is 2 to 1024. |
|---------------------------|--|

| | |
|------------------------|--|
| Command Default | The mode and the packet interval for a sampler are not configured. |
|------------------------|--|

| | |
|----------------------|-----------------------|
| Command Modes | Sampler configuration |
|----------------------|-----------------------|

| Command History | Release | Modification |
|------------------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | A total of four unique samplers are supported on the device. Packets are chosen in a manner that should eliminate any bias from traffic patterns and counter any attempt by users to avoid monitoring. |
|-------------------------|--|



| | |
|-------------|---|
| Note | The deterministic keyword is not supported, even though it is visible in the command-line help string. |
|-------------|---|

Examples

The following example enables random sampling with a window size of 1000:

```
Device(config)# sampler SAMPLER-1
Device(config-sampler)# mode random 1 out-of 1000
```

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 | | |
|---|--|--|
| <i>capture-name</i> | | The name of the capture to be defined. |
| interface <i>interface-type interface-id</i> | | Specifies an interface with <i>interface-type</i> and <i>interface-id</i> as an attachment point. The arguments have these meanings: <ul style="list-style-type: none"> • GigabitEthernet <i>interface-id</i>—A Gigabit Ethernet IEEE 802.3z interface. • vlan <i>vlan-id</i>—A VLAN. The range for <i>vlan-id</i> is 1 to 4095. |
| control-plane | | Specifies the control plane as an attachment point. |
| in out both | | Specifies the traffic direction to be captured. |

Command Default A Wireshark capture is not configured.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

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

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

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

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

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

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

Wireshark cannot capture packets on a destination SPAN port.

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

Examples

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

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



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

To define a capture point with multiple attachment points:

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

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

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

monitor capture buffer

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

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

Syntax Description

| | |
|--------------------------------|---|
| <i>capture-name</i> | 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 <i>buffer-size</i> | (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 Everest 16.5.1a | 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 clear 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 Everest 16.5.1a | 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
- — USB drive

Command Default

The captured packets are not stored.

Command Modes

Privileged EXEC

Command History

Release

Modification

This command was introduced.

Usage Guidelines

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

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



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

Example

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

monitor capture 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 | <i>capture-name</i> | The name of the capture to be modified. |
| | buffer-size <i>temp-buffer-size</i> | (Optional) Specifies the size of the temporary buffer. The range for <i>temp-buffer-size</i> is 1 to 100 MB. This is specified to reduce packet loss. |
| | location <i>file-location</i> : <i>file-name</i> | (Optional) Specifies the location and file name of the capture storage file. Acceptable values for <i>file-location</i> : <ul style="list-style-type: none"> • flash—On-board flash storage • — USB drive |
| | ring <i>number-of-ring-files</i> | (Optional) Specifies that the capture is to be stored in a circular file chain and the number of files in the file ring. |
| | size <i>total-size</i> | (Optional) Specifies the total size of the capture files. |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.5.1a | 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 | |
|----------------------------------|--|
| <i>capture-name</i> | The name of the capture to be assigned capture limits. |
| duration <i>seconds</i> | (Optional) Specifies the duration of the capture, in seconds. The range is from 1 to 1000000. |
| packet-length <i>size</i> | (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 <i>num</i> | (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 Everest 16.5.1a | 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

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 | | |
|--------------------|------------------------------------|---|
| | <i>capture-name</i> | The name of the capture to be assigned a core filter. |
| | any | Specifies all packets. |
| | mac <i>mac-match-string</i> | 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 Everest 16.5.1a | 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 pktlen-range

To specify a range of packet lengths for packet capture, use the **monitor capture pktlen-range** command in the EXEC configuration mode. To remove the packet length range filter, use the **no** form of this command

```
monitor capture capture-name interface interface-id {in | out | both} match pktlen-range [max
packet-length-in bytes ] [min packet-length-in bytes ]
no monitor capture capture-name interface interface-id {in | out | both} match pktlen-range [max
packet-length-in bytes ] [min packet-length-in bytes ]
```

| | |
|---------------------------|--|
| Syntax Description | <i>packet-length-in bytes</i> Defines the length of the packet to be captured. The range is from 1-9216. |
|---------------------------|--|

| | |
|------------------------|--|
| Command Default | The default action is to have no packet length range for packet capture. |
|------------------------|--|

| | |
|----------------------|----------------------------|
| Command Modes | Global configuration mode. |
|----------------------|----------------------------|

| | | |
|------------------------|-------------------------------|-----------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.3.1 | The command was introduced. |

This example shows how to define a range of packet lengths for packet capture. In this example the maximum length of packet is set to 100 bytes and the minimum length of packet is set to 50 bytes.

```
Device(config)#mon cap cap1 int FortyGigabitEthernet 1/0/1 in match pktlen-range max 100
min 50
```

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 | <i>capture-name</i> 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 Everest 16.5.1a | 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 Everest 16.5.1a | 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) or Encapsulated Remote Switched Port Analyzer (ERSPAN) session configuration for analyzing traffic between ports or add to an existing session configuration, use the **monitor session** global configuration command. To clear sessions, use the **no** form of this command.

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

| Syntax Description | | |
|--------------------|-----------------------------------|---|
| | <i>session-number</i> | The session number identified with the session. |
| | all | Clears all monitor sessions. |
| | local | Clears all local monitor sessions. |
| | range <i>session-range</i> | 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 Everest 16.5.1a | This command was introduced. |
| | Cisco IOS XE Gibraltar 16.11.1 | The type { erspan-destination erspan-source } keywords were 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, RSPAN, and ERSPAN 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, FRSPAN, and ERSPAN 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 | | |
|--------------------|--------------------------------------|---|
| | <i>session-number</i> | The session number identified with the SPAN |
| | interface <i>interface-id</i> | Specifies the destination or source interface for the session. Valid interface types include physical ports (including type, stack member, and channel), VLANs, and EtherChannels. EtherChannel channel is also a valid interface type, and the |
| | , | (Optional) Specifies a series of interfaces or VLANs from a previous range. Enter a space before a |
| | - | (Optional) Specifies a range of interfaces or VLANs from a previous range. Enter a space before a |
| | encapsulation replicate | (Optional) Specifies that the destination interface sends packets to the original destination. If not selected, the default is to send packets to the original destination. These keywords are valid only for local SPAN sessions. If not selected, the default is to send packets to the original VLAN ID; therefore, packets are always sent to the original destination. Ignored with the no form of the command. |
| | encapsulation dot1q | (Optional) Specifies that the destination interface sends packets with IEEE 802.1Q encapsulation. These keywords are valid only for local SPAN sessions. If not selected, the default is to send packets to the original VLAN ID; therefore, packets are always sent to the original destination. Ignored with the no form of the command. |
| | ingress | Enables ingress traffic forwarding. |
| | dot1q | (Optional) Accepts incoming packets with IEEE 802.1Q encapsulation. If not selected, the default is to accept packets with the default VLAN. |
| | untagged | (Optional) Accepts incoming packets with untagged frames. If not selected, the default is to accept packets with the default VLAN. |
| | isl | Specifies ingress forwarding using ISL encapsulation. |
| | remote | Specifies the remote VLAN for an RSPAN session. The remote VLAN must be in the range 1006 to 4094. The RSPAN VLAN cannot be VLAN 1 (the default for Token Ring and FDDI VLANs). |

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

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 Everest 16.5.1a | 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 | <i>session-number</i> | The session number identified with the SPAN or RSPAN session. |
| | vlan <i>vlan-id</i> | Specifies a list of VLANs as filters on trunk source ports to limit SPAN traffic to specific VLANs. The <i>vlan-id</i> range is 1 to 4094. |
| | , | (Optional) Specifies a series of VLANs, or separates a range of VLANs. 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 Everest 16.5.1a | 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:

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

monitor session source

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

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

| Syntax Description | | |
|--------------------------------------|--|---|
| <i>session_number</i> | | The session number identified with the SPAN or RSPAN session. The range is 1 to 66. |
| interface <i>interface-id</i> | | 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 <i>vlan-id</i> | | 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 Everest 16.5.1a | 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

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

```
monitor session span-session-number type {erspan-destination | erspan-source}
no monitor session span-session-number type {erspan-destination | erspan-source}
```

| | |
|---------------------------|---|
| Syntax Description | <i>span-session-number</i> Number of the local ERSPAN session. Valid values are from 1 to 66. |
|---------------------------|---|

Command Default ERSPAN source or destination session is not configured.

Command Modes Global configuration (config)

| Command History | Release | Modification |
|------------------------|--------------------------------|---|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |
| | Cisco IOS XE Gibraltar 16.11.1 | The erspan-destination keyword was introduced. |

Usage Guidelines The *span-session-number* and the session type 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.

A newly configured ERSPAN session will be in the **shutdown** state by default. The ERSPAN session remains inactive until the **no shutdown** command is configured along with other mandatory configurations such as source interface, ERSPAN ID, ERSPAN IP address, and so on.

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:

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

| Related Commands | Command | Description |
|-------------------------|--|---|
| | monitor session type | Creates an ERSPAN source or destination session number or enters the ERSPAN session configuration mode for the session. |
| | show capability feature monitor | Displays information about monitor features. |

| Command | Description |
|-----------------------------|--|
| show monitor session | Displays information about the ERSPAN, SPAN, and RSPAN sessions. |

option

To configure optional data parameters for a flow exporter for Flexible NetFlow, use the **option** command in flow exporter configuration mode. To remove optional data parameters for a flow exporter, use the **no** form of this command.

```
option {exporter-stats | interface-table | sampler-table} [{timeout seconds}]
no option {exporter-stats | interface-table | sampler-table}
```

| Syntax Description | | |
|--------------------|-------------------------------|--|
| | exporter-stats | Configures the exporter statistics option for flow exporters. |
| | interface-table | Configures the interface table option for flow exporters. |
| | sampler-table | Configures the export sampler table option for flow exporters. |
| | timeout <i>seconds</i> | (Optional) Configures the option resend time in seconds for flow exporters. The range is 1 to 86400. The default is 600. |

Command Default The timeout is 600 seconds. All other optional data parameters are not configured.

Command Modes Flow exporter configuration

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines The **option exporter-stats** command causes the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent. This command allows the collector to estimate packet loss for the export records it receives. The optional timeout alters the frequency at which the reports are sent.

The **option interface-table** command causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names. The optional timeout can alter the frequency at which the reports are sent.

The **option sampler-table** command causes the periodic sending of an options table, which details the configuration of each sampler and allows the collector to map the sampler ID provided in any flow record to a configuration that it can use to scale up the flow statistics. The optional timeout can alter the frequency at which the reports are sent.

To return this command to its default settings, use the **no option** or **default option** flow exporter configuration command.

The following example shows how to enable the periodic sending of the sampler option table, which allows the collector to map the sampler ID to the sampler type and rate:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option sampler-table
```

The following example shows how to enable the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option exporter-stats
```

The following example shows how to enable the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option interface-table
```

pae

To enable product telemetry collection, use the **pae** command in global configuration mode. To disable product telemetry collection, use the **no** form of this command.

pae
no pae

Command Default Product telemetry is enabled.

Command Modes Global configuration (config)

| Command History | Release | Modification |
|------------------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.11.1 | This command was introduced. |

Examples

The following example shows how to disable product telemetry collection:

```
Device> enable
Device# configure terminal
Device(config)# no pae
```

Related Commands

| Command | Description |
|--------------------------------------|--|
| show product-analytics kpi | Displays information about KPIs. |
| show product-analytics report | Displays reports and information about each report that is collected by product telemetry. |
| show product-analytics stats | Displays statistics and event history about each report. |

record

To add a flow record for a Flexible NetFlow flow monitor, use the **record** command in flow monitor configuration mode. To remove a flow record for a Flexible NetFlow flow monitor, use the **no** form of this command.

record *record-name*
no record

| | |
|---------------------------|---|
| Syntax Description | <i>record-name</i> Name of a user-defined flow record that was previously configured. |
|---------------------------|---|

| | |
|------------------------|----------------------------------|
| Command Default | A flow record is not configured. |
|------------------------|----------------------------------|

| | |
|----------------------|----------------------------|
| Command Modes | Flow monitor configuration |
|----------------------|----------------------------|

| Command History | Release | Modification |
|------------------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | Each flow monitor requires a record to define the contents and layout of its cache entries. The flow monitor can use one of the wide range of predefined record formats, or advanced users may create their own record formats. |
|-------------------------|---|



| | |
|-------------|--|
| Note | You must use the no ip flow monitor command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the record command for the flow monitor. |
|-------------|--|

Examples

The following example configures the flow monitor to use FLOW-RECORD-1:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# record FLOW-RECORD-1
```

sensor-name (stealthwatch-cloud-monitor)

To set the sensor name for the Stealthwatch Cloud registration, use the **sensor-name** *SwC-sensor-name* command in stealthwatch-cloud-monitor configuration mode.

sensor-name *SwC-sensor-name*

| | | |
|---------------------------|---|-------------------------------------|
| Syntax Description | <i>SwC-sensor-name</i> | Sensor name in alphanumeric format. |
| Command Default | The device name is configured. | |
| Command Modes | stealthwatch-cloud-monitor (stealthwatch-cloud-monitor) | |
| Command History | Release | Modification |
| | Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |

Usage Guidelines

Configure the **stealthwatch-cloud-monitor** command before setting the sensor name.

Setting the sensor name is optional. If no sensor name is set, by default, the device name is set as the sensor name.

Examples

The following example shows how to set the sensor name:

```
Device> enable
Device# configure terminal
Device(config)# stealthwatch-cloud-monitor
Device(config-stealthwatch-cloud-monitor)# service-key xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Device(config-stealthwatch-cloud-monitor)# sensor-name mysensor
```

| Related Commands | Command | Description |
|------------------|---|--|
| | service-key <i>SwC-service-key</i> | Configures the Stealthwatch Cloud service key. |
| | show stealth-watch-cloud detail | Displays the Stealthwatch Cloud registration status and its configured values. |
| | stealthwatch-cloud-monitor | Configures the Stealthwatch Cloud monitor. |
| | url <i>SwC-server-url</i> | Configures the Stealthwatch Cloud server URL. |

show flow monitor etta-mon cache

To display ETA monitor cache details, use the **show flow monitor etta-mon cache** command in privileged EXEC mode.

show flow monitor etta-mon cache

Command Default

None

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Example:

The following example shows how to display ETA flow monitor cache details:

```
Device>enable
Device#configure terminal
Device# show flow monitor etta-mon cache
Cache type: Normal (Platform cache)
Cache size: 10000
Current entries: 4
Flows added: 6
Flows aged: 2
- Inactive timeout ( 15 secs) 2
IPV4 DESTINATION ADDRESS: 15.15.15.35
IPV4 SOURCE ADDRESS: 72.163.128.140
IP PROTOCOL: 17
TRNS SOURCE PORT: 53
TRNS DESTINATION PORT: 12032
counter bytes long: 128
counter packets long: 1
timestamp abs first: 06:23:24.799
timestamp abs last: 06:23:24.799
interface input: Null
interface output: Null
```


sampler

To create a Flexible Netflow flow sampler, or to modify an existing Flexible Netflow flow sampler, and to enter Flexible Netflow sampler configuration mode, use the **sampler** command in global configuration mode. To remove a sampler, use the **no** form of this command.

```
sampler sampler-name
no sampler sampler-name
```

| | |
|---------------------------|---|
| Syntax Description | <i>sampler-name</i> Name of the flow sampler that is being created or modified. |
|---------------------------|---|

| | |
|------------------------|--|
| Command Default | Flexible Netflow flow samplers are not configured. |
|------------------------|--|

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

| Command History | Release | Modification |
|------------------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | Flow samplers are used to reduce the load placed by Flexible Netflow on the networking device to monitor traffic by limiting the number of packets that are analyzed. You configure a rate of sampling that is 1 out of a range of packets. Flow samplers are applied to interfaces in conjunction with a flow monitor to implement sampled Flexible Netflow. |
|-------------------------|---|

To enable flow sampling, you configure the record that you want to use for traffic analysis and assign it to a flow monitor. When you apply a flow monitor with a sampler to an interface, the sampled packets are analyzed at the rate specified by the sampler and compared with the flow record associated with the flow monitor. If the analyzed packets meet the criteria specified by the flow record, they are added to the flow monitor cache.

Examples

The following example creates a flow sampler name SAMPLER-1:

```
Device(config)# sampler SAMPLER-1
Device(config-sampler)#
```

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 Everest 16.5.1a | 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 class-map type control subscriber

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

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

| | | |
|---------------------------|---------------------------------------|---|
| Syntax Description | all | Displays class map statistics for all control policies. |
| | name <i>control-class-name</i> | Displays class map statistics for the specified control policy. |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

Examples

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

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

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

show flow exporter

To display flow exporter status and statistics, use the **show flow exporter** command in privileged EXEC mode.

```
show flow exporter [{export-ids netflow-v9} [name] exporter-name [{statistics | templates}] | statistics | templates}]
```

| Syntax Description | |
|------------------------------|---|
| export-ids netflow-v9 | (Optional) Displays the NetFlow Version 9 export fields that can be exported and their IDs. |
| name | (Optional) Specifies the name of a flow exporter. |
| <i>exporter-name</i> | (Optional) Name of a flow exporter that was previously configured. |
| statistics | (Optional) Displays statistics for all flow exporters or for the specified flow exporter. |
| templates | (Optional) Displays template information for all flow exporters or for the specified flow exporter. |

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

The following example displays the status and statistics for all of the flow exporters configured on a device:

```
Device# show flow exporter
Flow Exporter FLOW-EXPORTER-1:
  Description:           Exports to the datacenter
  Export protocol:       NetFlow Version 9
  Transport Configuration:
    Destination IP address: 192.168.0.1
    Source IP address:     192.168.0.2
    Transport Protocol:    UDP
    Destination Port:      9995
    Source Port:           55864
    DSCP:                  0x0
    TTL:                   255
    Output Features:       Used
```

This table describes the significant fields shown in the display:

Table 1: show flow exporter Field Descriptions

| Field | Description |
|---------------|--|
| Flow Exporter | The name of the flow exporter that you configured. |

| Field | Description |
|-------------------------|--|
| Description | The description that you configured for the exporter, or the default description User defined. |
| Transport Configuration | The transport configuration fields for this exporter. |
| Destination IP address | The IP address of the destination host. |
| Source IP address | The source IP address used by the exported packets. |
| Transport Protocol | The transport layer protocol used by the exported packets. |
| Destination Port | The destination UDP port to which the exported packets are sent. |
| Source Port | The source UDP port from which the exported packets are sent. |
| DSCP | The differentiated services code point (DSCP) value. |
| TTL | The time-to-live value. |
| Output Features | Specifies whether the output-features command, which causes the output features to be run on Flexible NetFlow export packets, has been used or not. |

The following example displays the status and statistics for all of the flow exporters configured on a device:

```
Device# show flow exporter name FLOW-EXPORTER-1 statistics
Flow Exporter FLOW-EXPORTER-1:
  Packet send statistics (last cleared 2w6d ago):
    Successfully sent:          0                (0 bytes)
```

show flow interface

To display the Flexible Netflow configuration and status for an interface, use the **show flow interface** command in privileged EXEC mode.

show flow interface [*type number*]

Syntax Description

type (Optional) The type of interface on which you want to display Flexible Netflow accounting configuration information.

number (Optional) The number of the interface on which you want to display Flexible Netflow accounting configuration information.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Examples

The following example displays the Flexible Netflow accounting configuration on Ethernet interfaces 0/0 and 0/1:

```
Device# show flow interface gigabitethernet1/0/1

Interface Ethernet1/0
  monitor:          FLOW-MONITOR-1
  direction:        Output
  traffic(ip):      on
Device# show flow interface gigabitethernet1/0/2
Interface Ethernet0/0
  monitor:          FLOW-MONITOR-1
  direction:        Input
  traffic(ip):      sampler SAMPLER-2#
```

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

Table 2: show flow interface Field Descriptions

| Field | Description |
|------------|--|
| Interface | The interface to which the information applies. |
| monitor | The name of the flow monitor that is configured on the interface. |
| direction: | The direction of traffic that is being monitored by the flow monitor. The possible values are: <ul style="list-style-type: none"> • Input—Traffic is being received by the interface. • Output—Traffic is being transmitted by the interface. |

| Field | Description |
|-------------|---|
| traffic(ip) | <p>Indicates if the flow monitor is in normal mode or sampler mode.</p> <p>The possible values are:</p> <ul style="list-style-type: none">• on—The flow monitor is in normal mode.• sampler—The flow monitor is in sampler mode (the name of the sampler will be included in the display). |

show flow monitor

To display the status and statistics for a Flexible NetFlow flow monitor, use the **show flow monitor** command in privileged EXEC mode.

| Syntax Description | name | (Optional) Specifies the name of a flow monitor. |
|--------------------|---------------------|--|
| | <i>monitor-name</i> | (Optional) Name of a flow monitor that was previously configured. |
| | cache | (Optional) Displays the contents of the cache for the flow monitor. |
| | format | (Optional) Specifies the use of one of the format options for formatting the display output. |
| | csv | (Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format. |
| | record | (Optional) Displays the flow monitor cache contents in record format. |
| | table | (Optional) Displays the flow monitor cache contents in table format. |
| | statistics | (Optional) Displays the statistics for the flow monitor. |

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines The **cache** keyword uses the record format by default.

The uppercase field names in the display output of the **show flowmonitor** *monitor-name* **cache** command are key fields that Flexible netFlow uses to differentiate flows. The lowercase field names in the display output of the **show flow monitor** *monitor-name* **cache** command are nonkey fields from which Flexible NetFlow collects values as additional data for the cache.

Examples

The following example displays the status for a flow monitor:

```
Device# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:      Used for basic traffic analysis
  Flow Record:     flow-record-1
  Flow Exporter:   flow-exporter-1
                  flow-exporter-2
  Cache:
    Type:          normal
    Status:        allocated
    Size:          4096 entries / 311316 bytes
    Inactive Timeout: 15 secs
    Active Timeout: 1800 secs
```

This table describes the significant fields shown in the display.

Table 3: show flow monitor monitor-name Field Descriptions

| Field | Description |
|------------------|---|
| Flow Monitor | Name of the flow monitor that you configured. |
| Description | Description that you configured or the monitor, or the default description User defined. |
| Flow Record | Flow record assigned to the flow monitor. |
| Flow Exporter | Exporters that are assigned to the flow monitor. |
| Cache | Information about the cache for the flow monitor. |
| Type | Flow monitor cache type. The value is always normal, as it is the only supported cache type. |
| Status | Status of the flow monitor cache. The possible values are: <ul style="list-style-type: none"> • allocated—The cache is allocated. • being deleted—The cache is being deleted. • not allocated—The cache is not allocated. |
| Size | Current cache size. |
| Inactive Timeout | Current value for the inactive timeout in seconds. |
| Active Timeout | Current value for the active timeout in seconds. |

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1:

This table describes the significant fields shown in the display.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1 in a table format:

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-IPv6 (the cache contains IPv6 data) in record format:

The following example displays the status and statistics for a flow monitor:

show flow record

To display the status and statistics for a Flexible Netflow flow record, use the **show flow record** command in privileged EXEC mode.

```
show flow record [{name] record-name}]
```

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | name (Optional) Specifies the name of a flow record. | |
| | <i>record-name</i> (Optional) Name of a user-defined flow record that was previously configured. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

The following example displays the status and statistics for FLOW-RECORD-1:

```
Device# show flow record FLOW-RECORD-1
flow record FLOW-RECORD-1:
  Description:      User defined
  No. of users:    0
  Total field space: 24 bytes
  Fields:
    match ipv6 destination address
    match transport source-port
    collect interface input
```

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 | | |
|--------------------|-------------------------|---|
| | <i>operation-number</i> | (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 Everest 16.5.1a | 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. |
| <i>session_number</i> | 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 <i>list</i> | (Optional) Displays a range of SPAN sessions, where <i>list</i> 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 Everest 16.5.1a | 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 encaps : DOT1Q
Session 2
-----
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/0/12
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encaps : Untagged

```

show monitor capture

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

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

| Syntax Description | | |
|---|--|------------------------------|
| capture-name | (Optional) Specifies the name of the capture to be displayed. | |
| buffer | (Optional) Specifies that a buffer associated with the named capture is to be displayed. | |
| file <i>file-location</i> : <i>file-name</i> | (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 <i>display-filter-string</i> | Filters the display content according to the <i>display-filter-string</i> . | |
| Command Default | Displays all capture content. | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Example

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

```
Device# show monitor capture mycap

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

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


show monitor session

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

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

| Syntax Description | | |
|--------------------|---------------------------|--|
| | <i>session_number</i> | The session number identified with the session. |
| | all | Displays all SPAN sessions. |
| | erspan-source | Displays only source ERSPAN sessions. |
| | erspan-destination | Displays only destination ERSPAN sessions. |
| | local | Displays only local SPAN sessions. |
| | range list | Displays a range of SPAN sessions. The range is defined by two numbers, or a range of sessions described by two numbers and a comma-separated list of parameters or identifiers. |
| | | Note This keyword is available only in Cisco IOS XE Gibraltar 16.11.1 and later releases. |
| | remote | Displays only remote SPAN sessions. |
| | detail | (Optional) Displays detailed information about the sessions. |

| Command Modes | |
|---------------|---------------------|
| | User EXEC (>) |
| | Privileged EXEC (#) |

| Command History | Release | Modification |
|-----------------|--------------------------------|---|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |
| | Cisco IOS XE Gibraltar 16.11.1 | The erspan-destination keyword 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 : Gi4/0/12
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged

```

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

```

Device# 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

```

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

```

Device# show monitor session erspan-destination

Type           : ERSPAN Destination Session
Status         : Admin Enabled
Source IP Address : 10.10.10.210
Source ERSPAN ID : 40

```

show parameter-map type subscriber attribute-to-service

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

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

| | | |
|---------------------------|---------------------------------------|--|
| Syntax Description | all | Displays statistics for all parameter maps. |
| | name <i>parameter-map-name</i> | Displays statistics for the specified parameter map. |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

Examples

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

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

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

show platform software et-analytics

To display et-analytics configuration, use the **show platform software et-analytics** command in privileged EXEC mode.

show platform software et-analytics {**global** | **interfaces**}

| Syntax Description | |
|--------------------|--|
| global | Displays global et-analytics configuration. |
| interfaces | Displays interface et-analytics configuration. |

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Example:

The following example shows how to display global et-analytics configuration:

```
Device>enable
Device#configure terminal
Device# show platform software et-analytics global
```

```
ET-Analytics Global state
=====
All Interfaces : Off
IP Flow-record Destination: 10.126.71.20 : 2055
Inactive timer: 0
ET-Analytics interfaces
GigabitEthernet1/0/3
```

The following example shows how to display global et-analytics configuration:

```
Device>enable
Device#configure terminal
Device# show platform software et-analytics interfaces
```

```
ET-Analytics interfaces
GigabitEthernet1/0/3
```

show platform software fed switch active fnf et-analytics-flow-dump

To display interface et-analytics flow dump, use the **show platform software fed switch active fnf et-analytics-flow-dump** command in privileged EXEC mode.

show platform software fed switch active fnf et-analytics-flow-dump

| | | |
|------------------------|------------------------------|------------------------------|
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Example:

The following example shows how to display interface et-analytics flow dump.:

```
Device>enable
Device#configure terminal
Device# show platform software fed switch active fnf et-analytics-flow-dump

ET Analytics Flow dump
=====
Total packets received (27)
Excess packets received (0)
(Index:0) 72.163.128.140, 15.15.15.35, protocol=17, source port=53, dest port=12032, flow
done=u
SPLT: len = 2, value = (25600,0) (128,0)
IDP: len = 128, value = 45:0:0:80:f0:6c:0:0:f9:11:
(Index:1) 72.163.128.140, 15.15.15.35, protocol=17, source port=53, dest port=32356, flow
done=u
SPLT: len = 2, value = (59649,0) (128,0)
IDP: len = 517, value = 45:0:2:5:c3:1:0:0:f9:11:
(Index:2) 15.15.15.35, 72.163.128.140, protocol=17, source port=12032, dest port=53, flow
done=u
SPLT: len = 2, value = (10496,0) (128,0)
IDP: len = 69, value = 45:0:0:45:62:ae:40:0:40:11:
(Index:3) 15.15.15.35, 72.163.128.140, protocol=17, source port=32356, dest port=53, flow
done=u
SPLT: len = 2, value = (10496,0) (128,0)
IDP: len = 69, value = 45:0:0:45:62:ad:40:0:40:11:
```

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 { <i>switch_num</i> active standby } | The device for which you want to display information. <ul style="list-style-type: none"> • <i>switch_num</i>—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 fed switch swc connection

To display the connection details and events of the Stealthwatch Cloud integration, use the **show platform software fed switch *switch-number* swc connection** command in privileged EXEC mode.

show platform software fed switch { *switch-number* | active } swc connection

| Syntax Description | |
|--|---|
| switch { <i>switch-number</i> active } | Displays switch information. <ul style="list-style-type: none"> • <i>switch_num</i>: Switch ID. • active : Displays information for the active switch. |
| swc connection | Displays the connection details and events. |

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |

Examples

The following is a sample output of the **show platform software fed switch active swc connection** command:

```
Device> enable
Device# show platform software fed switch active swc connection
Stealthwatch-Cloud details
  Registration
    #ID          : 0xc000001
    URL          : https://sensor.ext.obsrvbl.com
    Service Key  : XXXXXXXXXXXXXXXXXXXXXXXXXXXX
    Sensor Name  : C9200
    Registered   : N/A
  Connection
    Status       : DOWN
<<- Status will be in UP state only when the flow uploads into the Stealthwatch Cloud.
    Last status update : 02/09/2021 10:10:47
    # Flaps           : 0
    # Heartbeats      : 0
    # Lost heartbeats : 0
    Total RX bytes    : 7360
    Total TX bytes    : 869
    Upload Speed (B/s) : 127
    Download Speed (B/s) : 58
    # Open sessions   : 0
    # Redirections    : 0
    # Timeouts        : 0

  HTTP Events
    GET response      : 4
    GET request       : 4
    GET Status Code 2XX : 4
    PUT response      : 12
    PUT request       : 12
```



```

PUT Status Code 2XX           : 2
POST response                 : 2
POST request                  : 2
POST Status Code 2XX         : 2

API Events
TX                           : 4
OK                           : 2
Error                         : 2

Event History
Timestamp          #Times  Event                      RC Context
-----
02/10/2021 09:29:41.126 2      SEND_OK                    0 ID:0003
02/10/2021 09:29:39.795 2      SIGNAL_DATA                0 ID:0003
02/10/2021 09:29:38.279 12     PUT_DATA                   0 ID:0003
02/10/2021 09:29:37.962 4      GET_URL                    0 ID:0003
02/10/2021 09:29:37.961 4      SEND_START                 0 ID:0003
02/10/2021 09:27:41.484 2      SEND_ERR                   0 ID:0001
02/10/2021 09:27:41.484 2      MAX_ATTEMPTS               0 ID:0001
02/10/2021 09:22:53.670 4      REGISTER_OK                0 Not applicable
02/10/2021 09:22:53.670 4      SEND_ABORT_ALL             0 config change
02/10/2021 09:22:53.670 1      OPTIONS_CONFIG             0 File Extension: .csv.gz (reset)
02/10/2021 09:22:53.669 1      OPTIONS_CONFIG             0 Data Type: ios-xe-catalyst
02/10/2021 09:22:53.669 1      OPTIONS_CONFIG             0 URL: https://sensor.ext.obsrvbl.com
(res
02/10/2021 09:22:53.668 1      OPTIONS_CONFIG             0 Sensor Name: niinamdaUS (reset)
02/10/2021 09:22:53.553 1      OPTIONS_CONFIG             0 Service Key:
b5tQtXJM8AGZSp6oB8FvK4H0FiW

```

Related Commands

| Command | Description |
|--|---|
| clear platform software fed switch <i>{switch-number}</i> active }swc connection | Clears the connection details and events of the Stealthwatch Cloud integration. |
| show platform software fed switch <i>{switch-number}</i> active }swc statistics | Displays the statistical information of the Stealthwatch Cloud integration. |
| show stealth-watch-cloud detail | Displays the Stealthwatch Cloud registration status and its configured values. |
| stealthwatch-cloud-monitor | Configures the Stealthwatch Cloud monitor. |

show platform software fed switch swc statistics

To display the statistical information of the Stealthwatch Cloud integration, use the **show platform software fed switch *switch-number* swc statistics** command in privileged EXEC mode.

show platform software fed switch { *switch-number* | **active** } **swc statistics**

| Syntax Description | |
|--|--|
| switch { <i>switch-number</i> active } | Displays switch information. <ul style="list-style-type: none"> • <i>switch_num</i>: Switch ID. • active: Displays information for the active switch. |
| swc statistics | Displays the statistical information. |

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |

Examples

The following is a sample output of the **show platform software fed switch active swc statistics** command:

```
Device> enable
Device# show platform software fed switch active swc statistics
=====
SWC Upload Statistics:
=====
 1: Last file uploaded   : 202102100928_1
 2: Time of upload      : 02/10/21 09:29:41 UTC
 3: Current file uploading :
 4: Files queued for upload :
 5: Number of files queued : 0
 6: Last failed upload   :
 7: Files failed to upload : 0
 8: Files successfully uploaded : 1
=====
SWC File Creation Statistics:
=====
 9: Last file created    : 202102100929_1
10: Time of creation     : 02/10/21 09:29:08 UTC
=====
SWC Flow Statistics:
=====
11: Number of flows in prev file: 15
12: Number of flows in curr file: 11
13: Invalid dropped flows : 0
14: Error dropped flows : 0
=====
SWC Flags:
=====
15: Is Registered : Registered
16: Delete debug  : Disabled
```

```
17: Exporter delete debug : Disabled
18: Certificate Validation : Enabled
```

Related Commands

| Command | Description |
|--|---|
| clear platform software fed switch <i>{switch-number}</i> active }swc statistics | Clears the statistical information of the Stealthwatch Cloud integration. |
| show platform software fed switch <i>{switch-number}</i> active }swc connection | Displays the connection details and events of the Stealthwatch Cloud integration. |
| show stealth-watch-cloud detail | Displays the Stealthwatch Cloud registration status and its configured values. |
| stealthwatch-cloud-monitor | Configures the Stealthwatch Cloud monitor. |

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 <i>session-ID</i> | Displays information about the specified destination session. |
| source sess-id <i>session-ID</i> | Displays information about the specified source session. |

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|------------------------------|---|
| Cisco IOS XE Everest 16.5.1a | 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
```

show product-analytics kpi

To display information about the Key Performance Indicators (KPIs), use the **show product-analytics kpi** command in privileged EXEC mode.

show product-analytics kpi { **detail** | **report** | **summary** }

| Syntax Description | detail | report | summary |
|--------------------|---|---|---|
| | Displays detailed information about the KPIs. | Displays information about the KPIs from a specific report. | Displays summarized information about the KPIs. |

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.11.1 | This command was introduced. |

Example

The following example shows sample summarized information about KPIs:

```
Device> enable
Device# show product-analytics kpi summary
Product Analytics Engine KPIs
```

| Time | Report ID | KPI Name |
|---------------------|------------|-------------------|
| ----- | | |
| 12/26/2022 00:00:00 | 1672012800 | hardware_inventor |
| y_optics | | |
| 12/26/2022 00:00:00 | 1672012800 | hardware_inventor |
| y_no_optics | | |
| 12/27/2022 00:00:00 | 1672099200 | hardware_inventor |
| y_optics | | |
| 12/27/2022 00:00:00 | 1672099200 | hardware_inventor |
| y_no_optics | | |
| 12/28/2022 00:00:00 | 1672185600 | hardware_inventor |
| y_optics | | |
| 12/28/2022 00:00:00 | 1672185600 | hardware_inventor |
| y_no_optics | | |
| 12/29/2022 00:00:00 | 1672272000 | hardware_inventor |
| y_optics | | |

```

12/29/2022 00:00:00          1672272000          hardware_inventor
                             y_no_optics
12/30/2022 00:00:00          1672358400          hardware_inventor
                             y_optics
12/30/2022 00:00:00          1672358400          hardware_inventor

```

Related Commands

| Command | Description |
|--------------------------------------|--|
| pa | Enables product telemetry. |
| show product-analytics report | Displays reports and information about each report that is collected by product telemetry. |
| show product-analytics stats | Displays statistics and event history about each report. |

show product-analytics report

To display reports and information about each report that is collected by product telemetry, use the **show product-analytics report** command in privileged EXEC mode.

show product-analytics report { detail | summary }

| Syntax Description | detail | summary |
|--------------------|--|--|
| | Displays detailed information about the collected reports. | Displays summarized information about the collected reports. |

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.11.1 | This command was introduced. |

Examples

The following example shows summarized information about collected reports:

```
Device> enable
Device# show product-analytics report summary
Product Analytics Engine Reports
Time                               Report ID                               KPI Name
-----
04/21/2023 23:32:41                1682119961                             nat
04/21/2023 23:32:41                1682119961                             ipv6
04/21/2023 23:32:41                1682119961                             LAG_LACP
04/21/2023 23:32:41                1682119961                             Trustsec
04/21/2023 23:32:41                1682119961                             ISSU_mode
04/21/2023 23:32:41                1682119961                             install_mode
04/21/2023 23:32:41                1682119961                             memory_usage
04/21/2023 23:32:41                1682119961                             enabled_features
04/21/2023 23:32:41                1682119961                             global_CPU_usage
04/21/2023 23:32:41                1682119961                             software_packages
04/21/2023 23:32:41                1682119961                             app_guestshell_cfg
04/21/2023 23:32:41                1682119961                             hardware_inventory
04/21/2023 23:32:41                1682119961                             hardware_inventory_port_count
04/21/2023 23:33:18                1682119998                             nat
04/21/2023 23:33:18                1682119998                             ipv6
```



```

04/21/2023 23:33:18      1682119998      LAG_LACP
04/21/2023 23:33:18      1682119998      Trustsec
04/21/2023 23:33:18      1682119998      ISSU_mode
04/21/2023 23:33:18      1682119998      install_mode
04/21/2023 23:33:18      1682119998      memory_usage
04/21/2023 23:33:18      1682119998      enabled_features
04/21/2023 23:33:18      1682119998      global_CPU_usage
04/21/2023 23:33:18      1682119998      software_packages
04/21/2023 23:33:18      1682119998      app_guestshell_cfg
04/21/2023 23:33:18      1682119998      hardware_inventory
04/21/2023 23:33:18      1682119998      hardware_inventory_port_count

```

Related Commands

| Command | Description |
|-------------------------------------|--|
| pae | Enables product telemetry. |
| show product-analytics kpi | Displays information for KPIs. |
| show product-analytics stats | Displays statistics and event history about each report. |

show product-analytics stats

To display statistics and event history, use the **show product-analytics stats** command in privileged EXEC mode.

show product-analytics stats

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|-----------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.11.1 | This command was introduced. |

Examples

The following example shows the summarized information about the collected reports:

```

Device> enable
Device# show product-analytics stats
Product Analytics Engine Statistics

Policy-Version
  File version           : 1
  File path              : /usr/binos/conf/product_analytics/produ
                        ct_analytics_policy.json

Data-Store
  #Writes                : 8
  Total write time (us)  : 4118
  Average write time (us) : 514
  #Single Writes        : 200
  Total Single write time (us) : 2118
  Average Single write time (us) : 10
  #Queries              : 14
  Total query time (us)  : 10041
  Average query time (us) : 717
  #Query errors         :

Data-Source
  #Periodic reads       : 2
  Total periodic-read time (us) : 14339
  Average periodic-read time (us) : 7169
  #Periodic read batches : 6
  Total periodic-read-batch time (us) : 3193
  Average periodic-read-batch time (us) : 532
  #On-change reads     : 0

KPI
  #SQL computatious    : 0
  Total SQL KPI compute time (us) : 0
  Average SQL KPI compute time (us) : 0
  #LUA computatious    : 0
  Total LUA KPI compute time (us) : 0
  Average LUA KPI compute time (us) : 0

Event History
Timestamp          #Times  Event          RC Context
-----

```

```

-----
12/30/2022 00:02:56.630 36      DSRC_PERIOD_RD      0 /services;serviceName=io
      s_oper/platform_component
12/30/2022 00:02:56.629 24      DST_STORE_END      0
12/30/2022 00:02:56.628 24      DST_STORE_BEGIN    0
12/30/2022 00:02:56.628 24      DSRC_NORMALIZE     0 device_inventory

```

Counter

```

PAE_REPORT_SUCCESS           : 0
PAE_POLICY_PARSE_DISPATCH_FAILURE : 0
PAE_TDL_WATCH_POINT_ONCHANGE_FAILURE : 0
PAE_TDL_WATCH_POINT_PERIODIC_FAILURE : 0
PAE_TDL_RECORD_PROCESSING_FAILURE : 0
PAE_DSTORE_STORE_FAILURE    : 0
PAE_DSTORE_QUERY_FAILURE    : 0
PAE_DPROC_SQL_FAILURE       : 0
PAE_KPI_SQL_FAILURE         : 0
PAE_KPI_LUA_FAILURE         : 0
PAE_CRASH_WITH_BUILTIN_POLICY : 0
PAE_CRASH_WITH_DYNAMIC_POLICY : 0

```

Related Commands

| Command | Description |
|--------------------------------------|--|
| pae | Enables product telemetry. |
| show product-analytics kpi | Displays information for KPIs. |
| show product-analytics report | Displays reports and information about each report that is collected by product telemetry. |

show sampler

To display the status and statistics for a Flexible NetFlow sampler, use the **show sampler** command in privileged EXEC mode.

```
show sampler [{[name] sampler-name}]
```

| | |
|---------------------------|--|
| Syntax Description | name (Optional) Specifies the name of a sampler. |
| | <i>sampler-name</i> (Optional) Name of a sampler that was previously configured. |
| Command Default | None |
| Command Modes | Privileged EXEC |
| Command History | Release |
| | Modification |
| | Cisco IOS XE Everest 16.5.1a This command was introduced. |

The following example displays the status and statistics for all of the flow samplers configured:

```
Device# show sampler
Sampler SAMPLER-1:
  ID:                2083940135
  export ID:         0
  Description:       User defined
  Type:              Invalid (not in use)
  Rate:              1 out of 32
  Samples:           0
  Requests:          0
  Users (0):

Sampler SAMPLER-2:
  ID:                3800923489
  export ID:         1
  Description:       User defined
  Type:              random
  Rate:              1 out of 100
  Samples:           1
  Requests:          124
  Users (1):
    flow monitor FLOW-MONITOR-1 (datalink,vlan1) 0 out of 0
```

This table describes the significant fields shown in the display.

Table 4: show sampler Field Descriptions

| Field | Description |
|-----------|--------------------------------|
| ID | ID number of the flow sampler. |
| Export ID | ID of the flow sampler export. |

| Field | Description |
|-------------|---|
| Description | Description that you configured for the flow sampler, or the default description User defined. |
| Type | Sampling mode that you configured for the flow sampler. |
| Rate | Window size (for packet selection) that you configured for the flow sampler. The range is 2 to 32768. |
| Samples | Number of packets sampled since the flow sampler was configured or the device was restarted. This is equivalent to the number of times a positive response was received when the sampler was queried to determine if the traffic needed to be sampled. See the explanation of the Requests field in this table. |
| Requests | Number of times the flow sampler was queried to determine if the traffic needed to be sampled. |
| Users | Interfaces on which the flow sampler is configured. |

show snmp stats

To display the SNMP statistics, use the **show snmp stats** command in privileged EXEC mode.

```
show snmp stats { hosts | oid }
```

Syntax Description

hosts Displays the details of the SNMP servers polled to the SNMP agent.

oid Displays recently requested object identifiers (OIDs).

Command Default

Displays the SNMP manager entries polled to the SNMP agent.

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|-------------------------------|------------------------------|
| Cisco IOS XE Amsterdam 17.1.1 | This command was introduced. |

Usage Guidelines

Use the **show snmp stats hosts** command to list the NMS IP address, the number of times an NMS polls the agent, and the timestamp of polling. To delete the entries polled to the SNMP agent, use the **clear snmp stats hosts** command.

Before running the **show snmp stats oid** command, connect the device to the NMS. The command output displays the list of OIDs recently requested by the NMS. It also displays the number of times an object identifier is requested by the NMS. This information is useful for troubleshooting memory leaks and network failures when little information is available about the MIBs that the NMS is querying. You can use the **show snmp stats oid** command at any time to view OIDs recently requested by the NMS.

The following is sample output of the **show snmp stats hosts** command.

```
Device# show snmp stats hosts
Request Count      Last Timestamp      Address
2                  00:00:01 ago       3.3.3.3
1                  1w2d ago           2.2.2.2
```

The table below describes the significant fields shown in the display:

Table 5: show snmp stats hosts Field Descriptions

| Field | Description |
|----------------|--|
| Request Count | Displays the number of times an SNMP Manager has sent requests to the SNMP Agent. |
| Last Timestamp | Displays the time at which the request was sent to the SNMP Agent by the SNMP Manager. |

| Field | Description |
|---------|--|
| Address | Displays the IP Address of the SNMP Manager that has sent the request. |

The following is sample output of the **show snmp stats oid** command.

Device# **show snmp stats oid**

```

time-stamp                #of times requested      OID
15:30:01 UTC Dec 2 2019   6                        ifPhysAddress
15:30:01 UTC Dec 2 2019  10                       system.2
15:30:01 UTC Dec 2 2019   9                        system.1
09:39:39 UTC Nov 26 2019  3                        system.5
09:39:39 UTC Nov 26 2019  3                        stem.4
09:39:39 UTC Nov 26 2019  3                        system.7
09:39:39 UTC Nov 26 2019  2                        system.6
09:39:39 UTC Nov 26 2019 10                       ceemEventMapEntry.2
09:39:39 UTC Nov 26 2019  6                        ipAddrEntry.4
09:39:39 UTC Nov 26 2019  3                        ipAddrEntry.5
09:39:39 UTC Nov 26 2019 10                       ipAddrEntry.3
09:39:39 UTC Nov 26 2019  7                        ipAddrEntry.2
09:39:39 UTC Nov 26 2019  4                        ipAddrEntry.1
09:39:39 UTC Nov 26 2019  1                        lsystem.3

```

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

Table 6: show snmp stats oid Field Descriptions

| Field | Description |
|---------------------|---|
| time-stamp | Displays the time and date when the object identifiers is requested by the NMS. |
| #of times requested | Displays the number of times an object identifier is requested. |
| OID | Displays the object identifiers recently requested by the NMS. |

show stealth-watch-cloud detail

To display the status of the Stealthwatch Cloud registration details, use the **show stealth-watch-cloud detail** command in privileged EXEC mode.

show stealth-watch-cloud detail

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |

Examples

The following is a sample output of the **show stealth-watch-cloud detail** command:

```
Device> enable
Device# show stealth-watch-cloud detail
=====
Stealthwatch Cloud Parameters
=====
Service Key : XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Sensor Name : C9200
URL : https://sensor.eu-prod.obsrvbl.com
=====
Stealthwatch Cloud Sensor Info
=====
Sensor Status : Registered
Last heartbeat : 2020-08-21T10:35:16
```

Related Commands

| Command | Description |
|---|---|
| show platform software fed switch <i>{switch-number}</i> active }swc connection | Displays the connection details and events of the Stealthwatch Cloud integration. |
| show platform software fed switch <i>{switch-number}</i> active }swc statistics | Displays the statistics of the Stealthwatch Cloud integration. |
| stealthwatch-cloud-monitor | Configures the Stealthwatch Cloud monitor. |

shutdown (monitor session)

To disable a configured ERSPAN session, use the **shutdown** command in ERSPAN monitor source session configuration mode. To enable configured ERSPAN session, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

A newly configured ERSPAN session will be in the shutdown state.

Command Modes

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

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

The ERSPAN session remains inactive until the **no shutdown** command is configured.

Examples

The following example shows how to activate an ERSPAN session using the **no shutdown** command:

```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# description source1
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/1 rx
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# erspan-id 100
Device(config-mon-erspan-src-dst)# origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)# ip address 10.1.0.2
Device(config-mon-erspan-src-dst)# ip dscp 10
Device(config-mon-erspan-src-dst)# ip ttl 32
Device(config-mon-erspan-src-dst)# mtu 512
Device(config-mon-erspan-src-dst)# vrf monitoring
Device(config-mon-erspan-src-dst)# exit
Device(config-mon-erspan-src)# no shutdown
Device(config-mon-erspan-src)# end
```

Related Commands

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

snmp ifmib ifindex persist

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

snmp ifmib ifindex persist
no snmp ifmib ifindex persist

Syntax Description This command has no arguments or keywords.

Command Default The ifIndex persistence on a device is disabled.

Command Modes Global configuration (config)

Usage Guidelines The **snmp ifmib ifindex persist** command does not override an interface-specific configuration. The interface-specific configuration of ifIndex persistence is configured with the **snmp ifindex persist** and **snmp ifindex clear** commands in interface configuration mode.

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

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

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

Examples

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

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

Related Commands

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

snmp-server community

To configure the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in global configuration mode. To remove the specified community string, use the **no** form of this command.

```
snmp-server community [clear | encrypted] community-string [view
view-name] [RO | RW] [SDROwner | SystemOwner] [access-list-name]
no snmp-server community community-string
```

Syntax Description

| | |
|------------------------------|---|
| clear | (Optional) Specifies that the entered community-string is clear text and should be encrypted when displayed by the show running command. |
| encrypted | (Optional) Specifies that the entered <i>community-string</i> is encrypted text and should be displayed as such by the show running command. |
| <i>community-string</i> | Community string that acts like a password and permits access to the SNMP protocol. The maximum length of the <i>community-string</i> argument is 32 alphabetic characters. If the clear keyword was used, <i>community-string</i> is assumed to be clear text. If the encrypted keyword was used, <i>community-string</i> is assumed to be encrypted. If neither was used, <i>community-string</i> is assumed to be clear text. |
| view <i>view-name</i> | (Optional) Specifies the name of a previously defined view. The view defines the objects available to the community. |
| RO | (Optional) Specifies read-only access. Authorized management stations are able only to retrieve MIB objects. |
| RW | (Optional) Specifies read-write access. Authorized management stations are able both to retrieve and to modify MIB objects. |
| SDROwner | (Optional) Limits access to the owner service domain router (SDR). |
| SystemOwner | (Optional) Provides system-wide access including access to all non-owner SDRs. |
| <i>access-list-name</i> | (Optional) Name of an access list of IP addresses allowed to use the community string to gain access to the SNMP agent. |

Command Default

By default, an SNMP community string permits read-only access to all MIB objects. By default, a community string is assigned to the SDR owner.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------------------------|-----------------------------|
| Cisco IOS XE Everest 16.5.1a | The command was introduced. |

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **snmp-server community** command to configure the community access string to permit access to SNMP.

To remove the specified community string, use the **no** form of this command.

Use the **clear** keyword to specify that the clear text community string you enter is displayed encrypted in the **show running** command output. To enter an encrypted string, use the **encrypted** keyword. To enter a clear text community string that is not encrypted by the system, use neither of these keywords.

When the **snmp-server community** command is entered with the **SDROwner** keyword, SNMP access is granted only to the MIB object instances in the owner SDR. When the **snmp-server community** command is entered with the **SystemOwner** keyword, SNMP access is granted to all SDRs in the system.



Note In a non-owner SDR, a community name provides access only to the object instances that belong to that SDR, regardless of the access privilege assigned to the community name. Access to the owner SDR and system-wide access privileges are available only from the owner SDR.

Examples

This example shows how to assign the string comaccess to SNMP, allowing read-only access, and to specify that IP access list 4 can use the community string:

```
RP/0/RP0/CPU0:router(config)# snmp-server community comaccess ro 4
```

The following example shows how to assign the string mgr to SNMP, allowing read-write access to the objects in the restricted view:

```
RP/0/RP0/CPU0:router(config)# snmp-server community mgr view restricted rw
```

This example shows how to remove the community comaccess:

```
RP/0/RP0/CPU0:router(config)# no snmp-server community comaccess
```

Related Commands

| Command | Description |
|------------------|--|
| snmp-server view | Creates or updates an SNMP view entry. |

snmp-server enable traps

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

```
snmp-server enable traps [ auth-framework [ sec-violation ] | bridge | call-home |
config | config-copy | config-ctid | copy-config | cpu | dot1x | energywise | entity
| envmon | errdisable | event-manager | flash | fru-ctrl | mac-notification |
port-security | power-ethernet | rep | snmp | stackwise | storm-control | stpx |
syslog | transceiver | tty | vlan-membership | vlancreate | vlandelete | vstack |
vtp ]
```

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

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

| | |
|-------------------------|---|
| fru-ctrl | (Optional) Generates entity field-replaceable unit (FRU) control traps. In a device stack, this trap refers to the insertion or removal of a device in the stack. |
| 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 Everest 16.5.1a | This command was introduced. |
| Cisco IOS XE Dublin 17.11.1 | The license keyword was deprecated. There is no replacement keyword. |

Usage Guidelines

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

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

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



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



Note Informs are not supported in SNMPv1.

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

Examples

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

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

snmp-server enable traps bridge

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

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

Syntax Description

newroot (Optional) Enables SNMP STP bridge MIB new root traps.

topologychange (Optional) Enables SNMP STP bridge MIB topology change traps.

Command Default

The sending of bridge SNMP traps is disabled.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | 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 Everest 16.5.1a | 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 Everest 16.5.1a | 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 Everest 16.5.1a | 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 Everest 16.5.1a | 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 Everest 16.5.1a | 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
```

Examples

This example shows how to generate status-change traps:

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

snmp-server enable traps errdisable

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

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

| | | |
|---------------------------|---|--|
| Syntax Description | notification-rate <i>number-of-notifications</i> | (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 Everest 16.5.1a | 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 Everest 16.5.1a | 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 Everest 16.5.1a | 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 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

Cisco IOS XE Everest 16.5.1a

Modification

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. |
| <i>rate-limit-time</i> | (Optional) Specifies window of time in seconds for rate-limit traps. Accepted values are 2 to 60. |
| <i>max-number-of-traps</i> | (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 Everest 16.5.1a | 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 Everest 16.5.1a

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 <i>value</i> | (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 Everest 16.5.1a | 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 Everest 16.5.1a | 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 power-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 Everest 16.5.1a | 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 primary 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 Everest 16.5.1a | 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 | <p>trap-rate <i>number-of-minutes</i></p> <p>(Optional) Specifies the SNMP storm-control trap rate in minutes. Accepted values are from 0 to 1000. The default is 0.</p> <p>Value 0 indicates that no limit is imposed and a trap is sent at every occurrence. When configured, show run all command output displays <code>no snmp-server enable traps storm-control</code>.</p> |
|---------------------------|--|

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

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

| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Everest 16.5.1a | This command was introduced. |
|------------------------------|--|---------|--------------|------------------------------|------------------------------|
| Release | Modification | | | | |
| Cisco IOS XE Everest 16.5.1a | 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 Everest 16.5.1a | 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

a (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 Everest 16.5.1a | 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 Everest 16.5.1a | 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 Everest 16.5.1a | 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 <i>engineid-string</i> | 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 <i>ip-address</i> | Specifies the remote SNMP copy. Specify the <i>ip-address</i> of the device that contains the remote copy of SNMP. |
| udp-port <i>port-number</i> | (Optional) Specifies the User Datagram Protocol (UDP) port on the remote device. The default is 162. |

Command Modes

Global configuration

Command History

| Release | Modification |
|------------------------------|------------------------------|
| Cisco IOS XE Everest 16.5.1a | This command was introduced. |

Usage Guidelines

None

Examples

The following example configures a local engine ID of 123400000000000000000000:

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

snmp-server group

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

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

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

Syntax Description

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

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

Command Default

No SNMP server groups are configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

Configuring Notify Views

The notify-view option is available for two reasons:

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

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

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

- The **snmp-server host** command autogenerates a notify view for the user, and then adds it to the group associated with that user.
- Modifying the group's notify view will affect all users associated with that group.

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

1. **snmp-server user**—Configures an SNMP user.
2. **snmp-server group**—Configures an SNMP group, without adding a notify view .
3. **snmp-server host**—Autogenerates the notify view by specifying the recipient of a trap operation.

SNMP Contexts

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

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

Create an SNMP Group

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

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

Remove an SNMP Server Group

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

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

Associate an SNMP Server Group with Specified Views

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

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

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

Related Commands

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

snmp-server host

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

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

Syntax Description

| | |
|--|--|
| <i>host-addr</i> | Name or Internet address of the host (the targeted recipient). |
| vrf <i>vrf-instance</i> | (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). |
| <i>community-string</i> | 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.
 - **wireless**—Sends wireless traps.
-

Command Default

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

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

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

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



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

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

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

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

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

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

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

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

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

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

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

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

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

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

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

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

snmp-server manager

To start the Simple Network Management Protocol (SNMP) manager process, use the **snmp-server manager** command in global configuration mode. To stop the SNMP manager process, use the **no** form of this command.

snmp-server manager
no snmp-server manager

Command Default

Command Modes Global configuration (config)

Command History

| Release | Modification |
|------------------------------|-----------------------------|
| Cisco IOS XE Everest 16.5.1a | The command was introduced. |

Usage Guidelines

The SNMP manager process sends SNMP requests to agents and receives SNMP responses and notifications from agents. When the SNMP manager process is enabled, the router can query other SNMP agents and process incoming SNMP traps.

Most network security policies assume that routers will be accepting SNMP requests, sending SNMP responses, and sending SNMP notifications. With the SNMP manager functionality enabled, the router may also be sending SNMP requests, receiving SNMP responses, and receiving SNMP notifications. The security policy implementation may need to be updated prior to enabling this functionality.

SNMP requests are typically sent to UDP port 161. SNMP responses are typically sent from UDP port 161. SNMP notifications are typically sent to UDP port 162.

The following example shows how to enable the SNMP manager process:

```
Router(config)# snmp-server manager
```

Related Commands

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

snmp-server user

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

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

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

Syntax Description

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

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

Command Default

See the table in the “Usage Guidelines” section for default behaviors for encryption, passwords, and access lists.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

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

Table 7: snmp-server user Default Descriptions

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

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



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

Working with Passwords and Digests

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

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

Examples

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

Related Commands

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

snmp-server view

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

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

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

Command Default No view entry exists.

Command Modes Global configuration

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

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

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

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

Examples

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

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

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

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

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

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

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

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

Related Commands

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

source

To configure the source IP address interface for all of the packets sent by a Flexible Netflow flow exporter, use the **source** command in flow exporter configuration mode. To remove the source IP address interface for all of the packets sent by a Flexible Netflow flow exporter, use the **no** form of this command.

source *interface-type interface-number*
no source

| | | |
|---------------------------|--|---|
| Syntax Description | <i>interface-type</i> | Type of interface whose IP address you want to use for the source IP address of the packets sent by a Flexible Netflow flow exporter. |
| | <i>interface-number</i> | Interface number whose IP address you want to use for the source IP address of the packets sent by a Flexible Netflow flow exporter. |
| Command Default | The IP address of the interface over which the Flexible Netflow datagram is transmitted is used as the source IP address. | |
| Command Modes | Flow exporter configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.5.1a This command was introduced. | |
| Usage Guidelines | <p>The benefits of using a consistent IP source address for the datagrams that Flexible Netflow sends include the following:</p> <ul style="list-style-type: none"> • The source IP address of the datagrams exported by Flexible Netflow is used by the destination system to determine from which device the Flexible Netflow data is arriving. If your network has two or more paths that can be used to send Flexible Netflow datagrams from the device to the destination system and you do not specify the source interface from which the source IP address is to be obtained, the device uses the IP address of the interface over which the datagram is transmitted as the source IP address of the datagram. In this situation the destination system might receive Flexible Netflow datagrams from the same device, but with different source IP addresses. When the destination system receives Flexible Netflow datagrams from the same device with different source IP addresses, the destination system treats the Flexible Netflow datagrams as if they were being sent from different devices. To avoid having the destination system treat the Flexible Netflow datagrams as if they were being sent from different devices, you must configure the destination system to aggregate the Flexible Netflow datagrams it receives from all of the possible source IP addresses in the device into a single Flexible Netflow flow. • If your device has multiple interfaces that can be used to transmit datagrams to the destination system, and you do not configure the source command, you will have to add an entry for the IP address of each interface into any access lists that you create for permitting Flexible Netflow traffic. Creating and maintaining access lists for permitting Flexible Netflow traffic from known sources and blocking it from unknown sources is easier when you limit the source IP address for Flexible Netflow datagrams to a single IP address for each device that is exporting Flexible Netflow traffic. | |



Caution The interface that you configure as the **source** interface must have an IP address configured, and it must be up.



Tip When a transient outage occurs on the interface that you configured with the **source** command, the Flexible Netflow exporter reverts to the default behavior of using the IP address of the interface over which the datagrams are being transmitted as the source IP address for the datagrams. To avoid this problem, use a loopback interface as the source interface because loopback interfaces are not subject to the transient outages that can occur on physical interfaces.

To return this command to its default settings, use the **no source** or **default source** flow exporter configuration command.

Examples

The following example shows how to configure Flexible Netflow to use a loopback interface as the source interface for NetFlow traffic:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# source loopback 0
```


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 <i>type number</i> | Specifies an interface type and number. |
| vlan <i>vlan-ID</i> | 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 Everest 16.5.1a | 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:

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

| Related Commands | Command | Description |
|------------------|-----------------------------|--|
| | monitor session type | Configures a local ERSPAN source or destination session. |

socket

To specify the client socket and allow a TCL interpreter to connect via TCP over IPv4/IPv6 and open a TCP network connection use the **socket** command in the TCL configuration mode.

socket myaddr address myport port myvrf vrf-table-name host port

Syntax Description

myaddr Specifies domain name or numerical IP address of the client-side network interface required for the connection. Use this option especially if the client machine has multiple network interfaces.

myport Specifies port number that is required for the client's connection.

myvrf Specifies the vrf table name. If the vrf table is not configured, then the command will return a TCL_ERROR.

Command Default

Command Modes

TCL configuration mode

Command History

Release

Modification

Cisco IOS XE Amsterdam 17.2.1 The **myvrf** keyword was introduced.

stealthwatch-cloud-monitor

To configure the Stealthwatch Cloud monitor, use the **stealthwatch-cloud-monitor** command in global configuration mode.

stealthwatch-cloud-monitor

Command Default Stealthwatch Cloud is not configured.

Command Modes Global configuration (config)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |

Usage Guidelines Before configuring Stealthwatch Cloud monitor on a device, the following root certificates must be installed:

- Starfield Services Root certificate from <https://www.amazontrust.com/repository/%20SFC2CA-SFSRootCAG2.pem>
- Baltimore CyberTrust Root PEM certificate from <https://www.digicert.com/kb/digicert-root-certificates.htm>

After configuring Stealthwatch Cloud monitor on a device, configure the service key using the **service-key** *SwC-service-key* command.

Examples

The following example shows how to configure a Stealthwatch Cloud monitor:

```
Device> enable
Device# configure terminal
Device(config)# stealthwatch-cloud-monitor
Device(config-stealthwatch-cloud-monitor)#
```

| Related Commands | Command | Description |
|------------------|---|--|
| | sensor-name <i>SwC-sensor-name</i> | Sets the sensor name for the Stealthwatch Cloud registration. |
| | service-key <i>SwC-service-key</i> | Configures the Stealthwatch Cloud service key. |
| | show stealth-watch-cloud detail | Displays the Stealthwatch Cloud registration status and its configured values. |
| | url <i>SwC-server-url</i> | Configures the Stealthwatch Cloud server URL. |

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 Everest 16.5.1a | 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 <i>vlan_id</i> 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 Everest 16.5.1a Cisco IOS XE Fuji 16.9.1 | 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
```

ttl

To configure the time-to-live (TTL) value, use the **ttl** command in flow exporter configuration mode. To remove the TTL value, use the **no** form of this command.

```
ttl ttl
no ttl ttl
```

| | |
|---------------------------|--|
| Syntax Description | <i>ttl</i> Time-to-live (TTL) value for exported datagrams. The range is 1 to 255. The default is 255. |
|---------------------------|--|

| | |
|------------------------|----------------------------------|
| Command Default | Flow exporters use a TTL of 255. |
|------------------------|----------------------------------|

| | |
|----------------------|-----------------------------|
| Command Modes | Flow exporter configuration |
|----------------------|-----------------------------|

| Command History | Release | Modification |
|------------------------|------------------------------|------------------------------|
| | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | To return this command to its default settings, use the no ttl or default ttl flow exporter configuration command. |
|-------------------------|--|

The following example specifies a TTL of 15:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# ttl 15
```

transport

To configure the transport protocol for a flow exporter for Flexible Netflow, use the **transport** command in flow exporter configuration mode. To remove the transport protocol for a flow exporter, use the **no** form of this command.

```
transport udp udp-port
no transport udp udp-port
```

| Syntax Description | udp <i>udp-port</i> Specifies User Datagram Protocol (UDP) as the transport protocol and the UDP port number. | | | | |
|------------------------------|--|---------|--------------|------------------------------|------------------------------|
| Command Default | Flow exporters use UDP on port 9995. | | | | |
| Command Modes | Flow exporter configuration | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Everest 16.5.1a | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Everest 16.5.1a | This command was introduced. | | | | |
| Usage Guidelines | <p>To return this command to its default settings, use the no transport or default transport flow exporter configuration command.</p> <p>The following example configures UDP as the transport protocol and a UDP port number of 250:</p> <pre>Device(config)# flow exporter FLOW-EXPORTER-1 Device(config-flow-exporter)# transport udp 250</pre> | | | | |

template data timeout

To specify a timeout period for resending flow exporter template data, use the **template data timeout** command in flow exporter configuration mode. To remove the template resend timeout for a flow exporter, use the **no** form of this command.

template data timeout *seconds*
no template data timeout *seconds*

| | |
|---------------------------|---|
| Syntax Description | <i>seconds</i> Timeout value in seconds. The range is 1 to 86400. The default is 600. |
|---------------------------|---|

| | |
|------------------------|---|
| Command Default | The default template resend timeout for a flow exporter is 600 seconds. |
|------------------------|---|

| | |
|----------------------|-----------------------------|
| Command Modes | Flow exporter configuration |
|----------------------|-----------------------------|

| Command History | <table border="0" style="width: 100%;"> <tr> <th style="text-align: left;">Release</th> <th style="text-align: left;">Modification</th> </tr> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </table> | Release | Modification | Cisco IOS XE Everest 16.5.1a | This command was introduced. |
|------------------------------|---|---------|--------------|------------------------------|------------------------------|
| Release | Modification | | | | |
| Cisco IOS XE Everest 16.5.1a | This command was introduced. | | | | |

| | |
|-------------------------|---|
| Usage Guidelines | <p>Flow exporter template data describes the exported data records. Data records cannot be decoded without the corresponding template. The template data timeout command controls how often those templates are exported.</p> <p>To return this command to its default settings, use the no template data timeout or default template data timeout flow record exporter command.</p> |
|-------------------------|---|

The following example configures resending templates based on a timeout of 1000 seconds:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# template data timeout 1000
```


udp peek

To enable peeking into a UDP socket use the **udp_peek** command in the TCL configuration mode.

udp_peek *socket* **buffer-size** *buffer-size*

Syntax Description

buffer-size Specifies the buffer size.

Command Default**Command Modes**

TCL configuration mode

Command History**Release****Modification**

Cisco IOS XE Amsterdam 17.2.1 This command was introduced.

url (stealthwatch-cloud-monitor)

To configure the URL of the Stealthwatch Cloud portal, use the **url** *SwC-server-url* command in stealthwatch-cloud-monitor configuration mode.

url *SwC-server-url*

| | | |
|---------------------------|---|--------------------------------|
| Syntax Description | <i>SwC-server-url</i> | Stealthwatch Cloud server URL. |
| Command Default | The URL of the Stealthwatch Cloud server located in the U.S is configured. | |
| Command Modes | stealthwatch-cloud-monitor (stealthwatch-cloud-monitor) | |
| Command History | Release | Modification |
| | Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |
| Usage Guidelines | <p>Configuring the Stealthwatch Cloud URL is optional. Configure the stealthwatch-cloud-monitor and the service-key <i>SwC-service-key</i> commands before setting the Stealthwatch Cloud URL.</p> <p>If no URL is configured, by default, the URL of the Stealthwatch Cloud server, located in the U.S, is configured. Based on your location, the default URL redirects you to the nearest Stealthwatch Cloud server URL.</p> | |



Note All encrypted traffic must use HTTPS (TCP port 443) to reach the Stealthwatch Cloud portal.

Examples

The following example shows how to configure the URL of a Stealthwatch Cloud server:

```
Device> enable
Device# configure terminal
Device(config)# stealthwatch-cloud-monitor
Device(config-stealthwatch-cloud-monitor)# service-key xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Device(config-stealthwatch-cloud-monitor)# url https://sensors.eu-2.obsrvbl.com
```

Related Commands

| Command | Description |
|---|--|
| sensor-name <i>SwC-sensor-name</i> | Sets the sensor name for the Stealthwatch Cloud registration. |
| service-key <i>SwC-service-key</i> | Configures the Stealthwatch Cloud service key. |
| show stealth-watch-cloud detail | Displays the Stealthwatch Cloud registration status and its configured values. |
| stealthwatch-cloud-monitor | Configures the Stealthwatch Cloud monitor. |