Flexible NetFlow Commands

- cache, on page 3
- clear flow exporter, on page 5
- clear flow monitor, on page 6
- collect, on page 8
- collect counter, on page 9
- collect interface, on page 10
- collect timestamp absolute, on page 11
- collect transport tcp flags, on page 12
- datalink flow monitor, on page 13
- debug flow exporter, on page 14
- debug flow monitor, on page 15
- debug flow record, on page 16
- debug sampler, on page 17
- description, on page 18
- destination, on page 19
- dscp, on page 20
- export-protocol netflow-v9, on page 21
- export-protocol netflow-v5, on page 22
- exporter, on page 23
- flow exporter, on page 24
- flow monitor, on page 25
- flow record, on page 26
- ip flow monitor, on page 27
- ipv6 flow monitor, on page 29
- match datalink ethertype, on page 31
- match datalink mac, on page 32
- match datalink vlan, on page 33
- match flow cts, on page 34
- match flow direction, on page 35
- match interface, on page 36
- match ipv4, on page 37
- match ipv4 destination address, on page 38
- match ipv4 source address, on page 39

- match ipv4 ttl, on page 40
- match ipv6, on page 41
- match ipv6 destination address, on page 42
- match ipv6 hop-limit, on page 43
- match ipv6 source address, on page 44
- match transport, on page 45
- match transport icmp ipv4, on page 46
- match transport icmp ipv6, on page 47
- mode random 1 out-of, on page 48
- option, on page 49
- record, on page 51
- sampler, on page 52
- show flow exporter, on page 53
- show flow interface, on page 55
- show flow monitor, on page 57
- show flow record, on page 59
- show sampler, on page 60
- source, on page 62
- template data timeout, on page 64
- transport, on page 65
- ttl, on page 66

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** | **update**} *seconds* | **type** **normal**}
no **cache** {**timeout** {**active** | **inactive** | **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.
seconds	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 Gibraltar 16.11.1	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.
exporter-name	(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 Gibraltar 16.11.1	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.
monitor-name	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 Gibraltar 16.11.1	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
```

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 *collect counter*.
interface	Configures the input and output interface name as a non-key field for a flow record. For more information, see *collect interface*.
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 *collect timestamp absolute*.
transport	Enables the collecting of transport TCP flags from a flow record. For more information, see *collect transport tcp flags*.

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 Gibraltar 16.11.1	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 Gibraltar 16.11.1	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 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

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	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.

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 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 Gibraltar 16.11.1	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 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 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 Gibraltar 16.11.1	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
```

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

monitor-name	Name of the flow monitor to apply to the interface.
sampler *sampler-name*	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 Gibraltar 16.11.1	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.
exporter-name	(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.
number	(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 Gibraltar 16.11.1	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.
monitor-name	(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.
packets	(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 Gibraltar 16.11.1	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.
record-name	(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 Gibraltar 16.11.1	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

detailed	(Optional) Enables detailed debugging for sampler elements.
error	(Optional) Enables debugging for sampler errors.
name	(Optional) Specifies the name of a sampler.
sampler-name	(Optional) Name of a sampler that was previously configured.
sampling *samples*	(Optional) Enables debugging for sampling and specifies the number of samples to debug.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	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,O)
 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 Gibraltar 16.11.1	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
```

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 Gibraltar 16.11.1	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

dscp	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

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	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
```

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 Gibraltar 16.11.1	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 Gibraltar 16.11.1	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

exporter-name	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 Gibraltar 16.11.1	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
```

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

exporter-name	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 Gibraltar 16.11.1	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

monitor-name	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 Gibraltar 16.11.1	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

record-name	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 Gibraltar 16.11.1	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)#
```

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

monitor-name	Name of the flow monitor to apply to the interface.
sampler *sampler-name*	(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 Gibraltar 16.11.1	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

monitor-name	Name of the flow monitor to apply to the interface.
sampler *sampler-name*	(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 Gibraltar 16.11.1	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
```

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 Gibraltar 16.11.1	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

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 Gibraltar 16.11.1	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

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	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 vlan** command to create flows based on the unique VLAN IDs in the network traffic.

The following example configures the VLAN ID of traffic being 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 vlan input
```

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 Gibraltar 16.11.1	The 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 source group-tag as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match flow cts source group-tag
```

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 Gibraltar 16.11.1	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 Gibraltar 16.11.1	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 *match ipv4 destination address*.
protocol	Configures the IPv4 protocol as a key field.
source address	Configures the IPv4 destination address as a key field. For more information see *match ipv4 source address*.
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 Gibraltar 16.11.1	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 Gibraltar 16.11.1	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 Gibraltar 16.11.1	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

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	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 *match ipv6 destination address*.
protocol	Configures the IPv6 protocol as a key field.
source address	Configures the IPv4 destination address as a key field. For more information see *match ipv6 source address*.

Command Default

The IPv6 fields are not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	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 Gibraltar 16.11.1	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 Gibraltar 16.11.1	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

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	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
```

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 Gibraltar 16.11.1	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:

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

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

```
Device(config)# flow record FLOW-RECORD-1
Device(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 Gibraltar 16.11.1	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 Gibraltar 16.11.1	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
```

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

window-size	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 Gibraltar 16.11.1	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
```

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 *seconds*	(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 Gibraltar 16.11.1	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
```

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

record-name	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 Gibraltar 16.11.1	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
```

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

sampler-name	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 Gibraltar 16.11.1	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 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.
exporter-name	(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 Gibraltar 16.11.1	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 Gibraltar 16.11.1	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: • Input—Traffic is being received by the interface. • Output—Traffic is being transmitted by the interface.

Field	Description
traffic(ip)	Indicates if the flow monitor is in normal mode or sampler mode. The possible values are: • 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.
monitor-name	(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 Gibraltar 16.11.1	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: • 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.
record-name	(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 Gibraltar 16.11.1	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 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.
sampler-name	(Optional) Name of a sampler that was previously configured.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	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.

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

interface-type	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.
interface-number	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 Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

The benefits of using a consistent IP source address for the datagrams that Flexible Netflow sends include the following:

- 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
```

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

seconds	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

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

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.

To return this command to its default settings, use the **no template data timeout** or **default template data timeout** flow record exporter command.

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
```

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 *udp-port*	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

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

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

The following example configures UDP as the transport protocol and a UDP port number of 250:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# transport udp 250
```

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

ttl	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 Gibraltar 16.11.1	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
```