# Configuring Flexible NetFlow


- Prerequisites for Flexible NetFlow, on page 1
- Restrictions for Flexible NetFlow, on page 2
- Information About Flexible Netflow, on page 4
- How to Configure Flexible Netflow, on page 10
- Monitoring Flexible NetFlow, on page 21
- Configuration Examples for Flexible NetFlow, on page 21
- Additional References for NetFlow, on page 22
- Feature Information for Flexible NetFlow, on page 23


## Prerequisites for Flexible NetFlow

- Flexible NetFlow is supported on the Catalyst 2960-X Switch and the Catalyst 2960-XR Switch with a Cisco ONE for Access license. Catalyst 2960-XR is not stackable with the Catalyst 2960-X platform.
- One of the following must be enabled on your device and on any interfaces on which you want to enable Flexible NetFlow: Cisco Express Forwarding or distributed Cisco Express Forwarding.
- The targets for attaching a NetFlow monitor are the following:
  - Port—Monitor attachment is only supported on physical interfaces and not on logical interfaces, such as EtherChannels. The physical interface could be a routed port or a switched port.
  - VLAN—Monitor attachment is supported on VLAN interfaces only (SVI) and not on a Layer 2 VLAN.
- You are familiar with the Flexible NetFlow key fields as they are defined in the following commands:
  - **match datalink**—Datalink (layer2) fields
  - **match ipv4**—IPv4 fields
  - **match ipv6**—IPv6 fields
  - **match transport**—Transport layer fields
- You are familiar with the Flexible NetFlow non key fields as they are defined in the following commands:
  - **collect counter**—Counter fields

- **collect flow**—Flow identifying fields
- **collect interface**—Interface fields
- **collect timestamp**—Timestamp fields
- **collect transport**—Transport layer fields

# Restrictions for Flexible NetFlow

The following restrictions apply to Flexible NetFlow and Flexible NetFlow Lite:

General Restrictions:

- InterSwitch Link (ISL) is not supported.
- Policy-based NetFlow is not supported.
- Cisco TrustSec monitoring is not supported.
- Access control lists (ACL)-based NetFlow is not supported.
- Only NetFlow Version 9 is supported for Flexible NetFlow exporter using the *export-protocol* command option.
- NetFlow Version 5 is not supported.

Flow Record Restrictions:

- When a flow monitor has configured the **collect interface output** command as the collect field in the flow record, the field will return a value of **NULL** when a flow gets created for any of the following addresses:
  - L2 broadcast and multicast
  - L3 broadcast and multicast
  - L2 unknown destination.

  When a flow monitor has the collect interface output configured as the collect field in the flow record, the output interface is detected based on the destination IP address on the device. For the different flow monitors, you must configure the following commands:
  - IPv4 flow monitor--Configure the **match ipv4 destination address** command.
  - IPv6 flow monitor--Configure the **match ipv6 destination address** command.
  - Datalink flow monitor--Configure the **match datalink mac destination address input** command.
- Predefined flow records are not supported.

Monitor Restrictions:

- Monitor attachment is only supported in the ingress direction.
- One monitor per interface is supported, although multiple exporters per interface are supported.

- Only permanent and normal cache is supported for the monitor; immediate cache is not supported.
- Changing any monitor parameter will not be supported when it is applied on any of the interfaces or VLANs.
- When both the port and VLANs have monitors attached, then VLAN monitor will overwrite the port monitor for traffic coming on the port.
- Flow monitor type and traffic type (type means IPv4, IPv6, and data link) should be same for the flows to be created.
- You cannot attach an IP and a port-based monitor to an interface. A 48-port device supports a maximum of 48 monitors (IP or port-based) and for 256 SVIs, you can configure up to 256 monitors (IP or port-based).
- When running the **show flow monitor** *flow_name* **cache** command, the device displays cache information from an earlier switch software version (Catalyst 2960-S) with all fields entered as zero. Ignore these fields, as they are inapplicable to the switch.

Sampler Restrictions:

- For both port and VLANS, a total of only 4 samplers (random or deterministic) are supported on the device.
- The sampling minimum rate for both modes is 1 out of 32 flows, and the sampling maximum rate for both modes is 1 out of 1022 flows.
- Use the **ip flow monitor** *monitor_name* sampler *sampler_name* **input** command to associate a sampler with a monitor while attaching it to an interface.
- When you attach a monitor using a deterministic sampler, every attachment with the same sampler uses one new free sampler from the switch (hardware) out of the 4 available samplers. You are not allowed to attach a monitor with any sampler, beyond 4 attachments.

  When you attach a monitor using a random sampler, only the first attachment uses a new sampler from the switch (hardware). The remainder of all of the attachments using the same sampler, share the same sampler.

  Because of this behavior, when using a deterministic sampler, you can always make sure that the correct number of flows are sampled by comparing the sampling rate and what the device sends. If the same random sampler is used with multiple interfaces, flows from any interface can always be sampled, and flows from other interfaces can always be skipped.

Stacking Restrictions:

- Each device in a stack (hardware) can support the creation of a maximum of 16,000 flows at any time. But as the flows are periodically pushed to the software cache, the software cache can hold a much larger amount of flows (1048 Kb flows). From the hardware flow cache, every 20 seconds (termed as poll timer), 200 flows (termed as poll entries) are pushed to software.
  - Use the **remote command all show platform hulc-fnf poll** command to report on the current NetFlow polling parameters of each switch.
  - Use the **show platform hulc-fnf poll** command to report on the current NetFlow polling parameters of the active switch.
- Network flows and statistics are collected at the line rate.

# Information About Flexible Netflow

## Flexible NetFlow Overview

Flexible NetFlow uses flows to provide statistics for accounting, network monitoring, and network planning.

A flow is a unidirectional stream of packets that arrives on a source interface and has the same values for the keys. A key is an identified value for a field within the packet. You create a flow using a flow record to define the unique keys for your flow.

The switch supports the Flexible NetFlow feature that enables enhanced network anomalies and security detection. Flexible NetFlow allows you to define an optimal flow record for a particular application by selecting the keys from a large collection of predefined fields.

All key values must match for the packet to count in a given flow. A flow might gather other fields of interest, depending on the export record version that you configure. Flows are stored in the Flexible NetFlow cache.

You can export the data that Flexible NetFlow gathers for your flow by using an exporter and export this data to a remote system such as a Flexible NetFlow collector. The Flexible NetFlow collector can use an IPv4 address.

You define the size of the data that you want to collect for a flow using a monitor. The monitor combines the flow record and exporter with the Flexible NetFlow cache information.

## Original NetFlow and Benefits of Flexible NetFlow

Flexible NetFlow allows the flow to be user defined. The benefits of Flexible NetFlow include:

- High-capacity flow recognition, including scalability and aggregation of flow information.
- Enhanced flow infrastructure for security monitoring and dDoS detection and identification.
- New information from packets to adapt flow information to a particular service or operation in the network. The flow information available will be customizable by Flexible NetFlow users.
- Extensive use of Cisco’s flexible and extensible NetFlow Version 9.
- A comprehensive IP accounting feature that can be used to replace many accounting features, such as IP accounting, Border Gateway Protocol (BGP) Policy Accounting, and persistent caches.
- Supports Unicast, Multicast and Broadcast traffic and flows for these traffic is added.

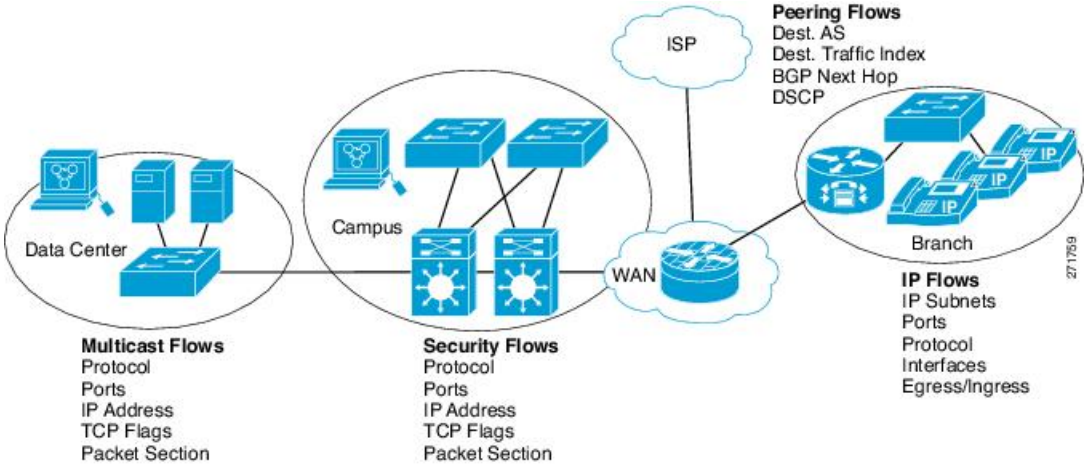
Flexible NetFlow allows you to understand network behavior with more efficiency, with specific flow information tailored for various services used in the network. The following are some example applications for a Flexible NetFlow feature:

- Flexible NetFlow enhances Cisco NetFlow as a security monitoring tool. For instance, new flow keys can be defined for packet length or MAC address, allowing users to search for a specific type of attack in the network.
- Flexible NetFlow allows you to quickly identify how much application traffic is being sent between hosts by specifically tracking TCP or UDP applications by the class of service (CoS) in the packets.

- The accounting of traffic entering a Multiprotocol Label Switching (MPLS) or IP core network and its destination for each next hop per class of service. This capability allows the building of an edge-to-edge traffic matrix.

The figure below is an example of how Flexible NetFlow might be deployed in a network.

***Figure 1: Typical Deployment for Flexible NetFlow***




# Flexible NetFlow Components

Flexible NetFlow consists of components that can be used together in several variations to perform traffic analysis and data export. The user-defined flow records and the component structure of Flexible NetFlow facilitates the creation of various configurations for traffic analysis and data export on a networking device with a minimum number of configuration commands. Each flow monitor can have a unique combination of flow record, flow exporter, and cache type. If you change a parameter such as the destination IP address for a flow exporter, it is automatically changed for all the flow monitors that use the flow exporter. The same flow monitor can be used in conjunction with different flow samplers to sample the same type of network traffic at different rates on different interfaces. The following sections provide more information on Flexible NetFlow components:

## Flow Records

In Flexible NetFlow a combination of key and nonkey fields is called a record. Flexible NetFlow records are assigned to Flexible NetFlow flow monitors to define the cache that is used for storing flow data.

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 switch 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. The switch enables the following match fields as the defaults when you create a flow record:

- match datalink—Layer 2 attributes
- match ipv4—IPv4 attributes
- match ipv6—IPv6 attributes
- match transport—Transport layer fields

- match wireless—Wireless fields

### User-Defined Records

Flexible NetFlow enables you to define your own records for a Flexible NetFlow flow monitor cache by specifying the key and nonkey fields to customize the data collection to your specific requirements. When you define your own records for a Flexible NetFlow flow monitor cache, they are referred to as *user-defined records*. 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. Flexible NetFlow enables you to capture counter values such as the number of bytes and packets in a flow as nonkey fields.

Flexible NetFlow adds a new Version 9 export format field type for the header and packet section types. Flexible NetFlow will communicate to the NetFlow collector the configured section sizes in the corresponding Version 9 export template fields. The payload sections will have a corresponding length field that can be used to collect the actual size of the collected section.

## Flow Exporters

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.

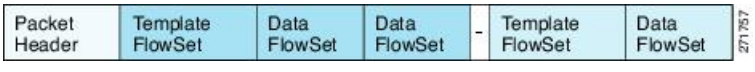
### NetFlow Data Export Format Version 9

The basic output of NetFlow is a flow record. Several different formats for flow records have evolved as NetFlow has matured. The most recent evolution of the NetFlow export format is known as Version 9. The distinguishing feature of the NetFlow Version 9 export format is that it is template-based. Templates provide an extensible design to the record format, a feature that should allow future enhancements to NetFlow services without requiring concurrent changes to the basic flow-record format. Using templates provides several key benefits:

- Third-party business partners who produce applications that provide collector or display services for NetFlow do not have to recompile their applications each time a new NetFlow feature is added. Instead, they should be able to use an external data file that documents the known template formats.
- New features can be added to NetFlow quickly without breaking current implementations.
- NetFlow is “future-proofed” against new or developing protocols because the Version 9 format can be adapted to provide support for them.

The Version 9 export format consists of a packet header followed by one or more template flow or data flow sets. A template flow set provides a description of the fields that will be present in future data flow sets. These data flow sets may occur later within the same export packet or in subsequent export packets. Template flow and data flow sets can be intermingled within a single export packet, as illustrated in the figure below.

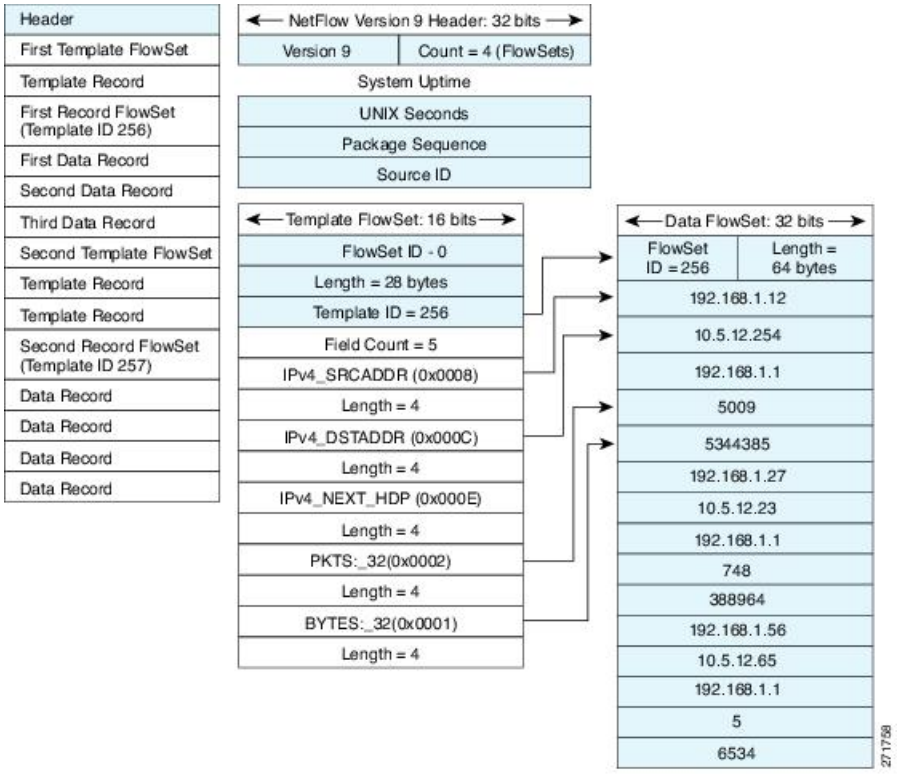
***Figure 2: Version 9 Export Packet***




NetFlow Version 9 will periodically export the template data so the NetFlow collector will understand what data is to be sent and also export the data flow set for the template. The key advantage to Flexible NetFlow

is that the user configures a flow record, which is effectively converted to a Version 9 template and then forwarded to the collector. The figure below is a detailed example of the NetFlow Version 9 export format, including the header, template flow, and data flow sets.

***Figure 3: Detailed Example of the NetFlow Version 9 Export Format***



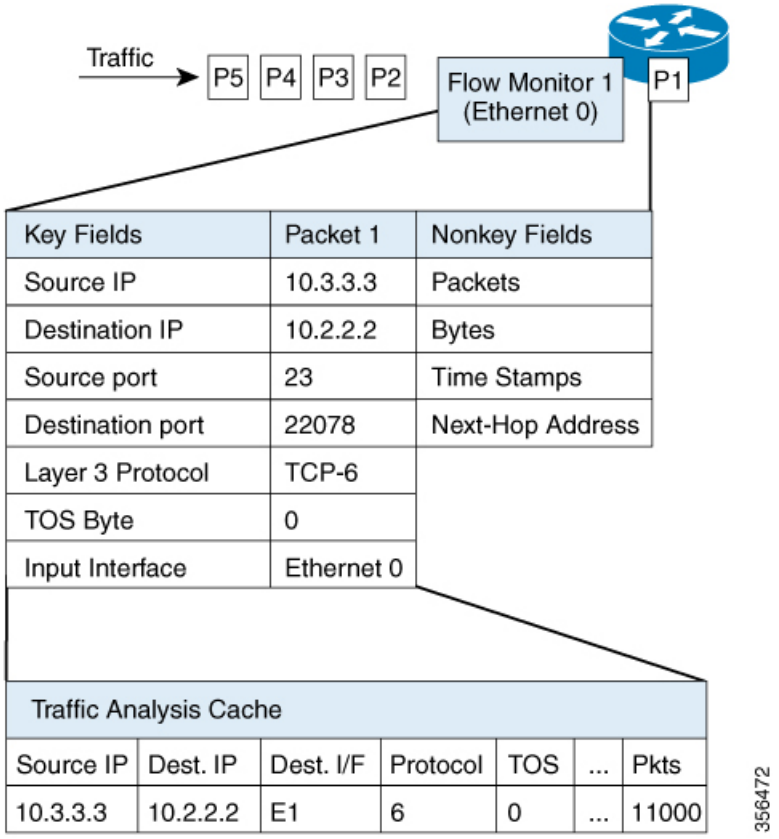

## Flow Monitors

Flow monitors are the Flexible NetFlow component that is applied to interfaces to perform network traffic monitoring.

Flow data is collected from the network traffic and added to the flow monitor cache during the monitoring process based on the key and nonkey fields in the flow record.

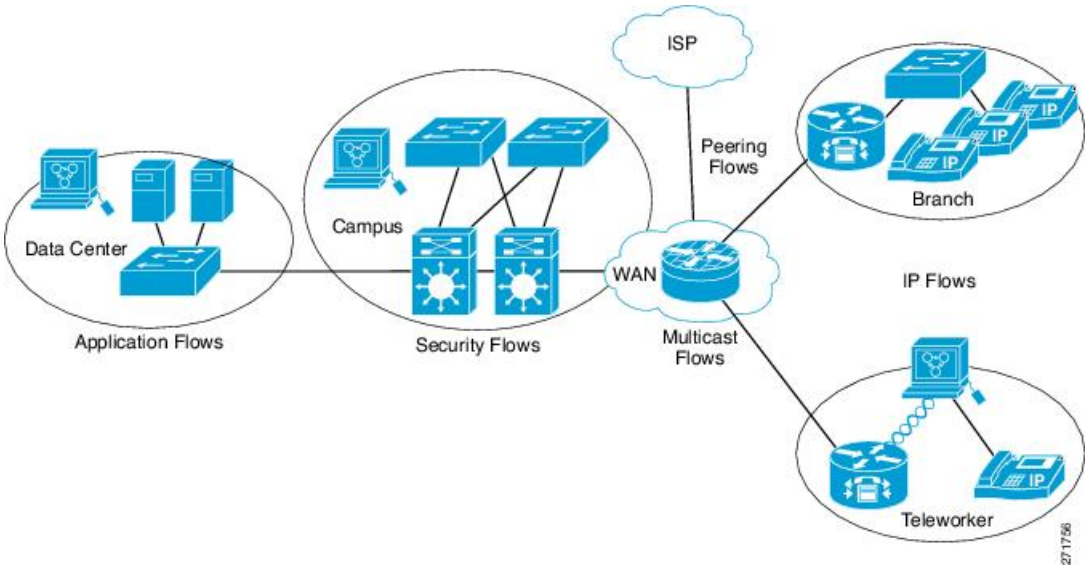
Flexible NetFlow can be used to perform different types of analysis on the same traffic. In the figure below, packet 1 is analyzed using a record designed for standard traffic analysis on the input interface

*Figure 4: Example of Using a Flow Monitor to Analyze Incoming Traffic*




The figure below shows a more complex example of how you can apply different types of flow monitors with custom records.

*Figure 5: Complex Example of Using Multiple Types of Flow Monitors with Custom Records*



#### Normal

The default cache type is “normal”. In this mode, the entries in the cache are aged out according to the timeout active and timeout inactive settings. When a cache entry is aged out, it is removed from the cache and exported via any exporters configured.

## Flow Samplers

Flow samplers are created as separate components in a router’s configuration. Flow samplers are used to reduce the load on the device that is running Flexible NetFlow by limiting the number of packets that are selected for analysis.

Samplers use random sampling techniques (modes); that is, a randomly selected sampling position is used each time a sample is taken.

Flow sampling exchanges monitoring accuracy for router performance. When you apply a sampler to a flow monitor, the overhead load on the router of running the flow monitor is reduced because the number of packets that the flow monitor must analyze is reduced. The reduction in the number of packets that are analyzed by the flow monitor causes a corresponding reduction in the accuracy of the information stored in the flow monitor’s cache.

Samplers are combined with flow monitors when they are applied to an interface with the **ip flow monitor** command.

# Supported Flexible NetFlow Fields

The following is the list of supported key fields in Flexible NetFlow:

- Source MAC and Destination MAC
- Datalink EtherType
- IPv4 source address
- IPv4 destination address
- IPv6 source address
- IPv6 destination address
- IPv4 TOS
- IPv6 traffic-class
- IPv6 flow label
- IPv4 protocol
- IPv6 protocol
- Layer 4 source port
- Layer 4 destination port

The following is the list of supported non-key fields in Flexible NetFlow:

- Interface input
- Interface output

- Bytes long
- Packets long
- Timestamp absolute first
- Timestamp absolute last
- Cumulative TCP flag
- Sampler ID

# Default Settings

The following table lists the Flexible NetFlow default settings for the switch.

***Table 1: Default Flexible NetFlow Settings***

| Setting | Default |
|---|---|
| Flow active timeout | 1800 seconds<br>**Note** The default value for this setting may be too high for your specific Flexible NetFlow configuration. You may want to consider changing it to a lower value of 180 or 300 seconds. |
| Flow timeout inactive | Enabled, 30 seconds |
| Flow update timeout | 1800 seconds |
| Default cache size | 16640 entries |

In Cisco IOS Release 15.2(5)E1, Flexible NetFlow polling was changed from 200 entries every 20 seconds to 2000 entries every 5 seconds. Based on this change, the current flow count will reflect the actual hardware flow count, and continuously active flows will experience active timeout. All flows will be exported as per the configured timeout values.

# How to Configure Flexible Netflow

To configure Flexible Netflow, follow these general steps:

1. Create a flow record by specifying keys and non-key fields to the flow.
2. Create an optional flow exporter by specifying the protocol and transport destination port, destination, and other parameters.
3. Create a flow monitor based on the flow record and flow exporter.
4. Create an optional sampler.
5. Apply the flow monitor to a Layer 2 port, Layer 3 port, or VLAN.

# Creating a Flow Record

Perform this task to configure a customized flow record.

Customized flow records are used to analyze traffic data for a specific purpose. A customized flow record must have at least one **match** criterion for use as the key field and typically has at least one **collect** criterion for use as a nonkey field.

There are hundreds of possible permutations of customized flow records. This task shows the steps that are used to create one of the possible permutations. Modify the steps in this task as appropriate to create a customized flow record for your requirements.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **flow record** *record-name*<br>**Example:**<br>`Device(config)# flow record FLOW-RECORD-1` | Creates a flow record and enters Flexible NetFlow flow record configuration mode.<br>• This command also allows you to modify an existing flow record. |
| **Step 4** | **description** *description*<br>**Example:**<br>`Device(config-flow-record)# description Used for basic traffic analysis` | (Optional) Creates a description for the flow record. |
| **Step 5** | **match** {**ipv4** \| **ipv6**} {**destination** \| **source**} **address**<br>**Example:**<br>`Device(config-flow-record)# match ipv4 destination address` | **Note** This example configures the IPv4 destination address as a key field for the record. For information about the other key fields available for the **match ipv4** command, and the other **match** commands that are available to configure key fields. |
| **Step 6** | Repeat Step 5 as required to configure additional key fields for the record. | — |
| **Step 7** | Choose the required collect fields:<br>• **collect counter** {**bytes** [**permanent** \| **long**] \| **packets** }[**permanent** \| **long**] | Configures the number of bytes as a nonkey field for the record. |

| | Command or Action | Purpose |
|---|---|---|
| | • **collect timestamp sys-uptime** {**first** \| **last**}<br>**Example:**<br>`Device(config-flow-record)# collect counter bytes long` | |
| **Step 8** | Repeat the above step as required to configure additional nonkey fields for the record. | — |
| **Step 9** | **end**<br>**Example:**<br>`Device(config-flow-record)# end` | Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode. |
| **Step 10** | **show flow record** *record-name*<br>**Example:**<br>`Device# show flow record FLOW_RECORD-1` | (Optional) Displays the current status of the specified flow record. |
| **Step 11** | **show running-config flow record** *record-name*<br>**Example:**<br>`Device# show running-config flow record FLOW_RECORD-1` | (Optional) Displays the configuration of the specified flow record. |

# Creating a Flow Exporter

You can create a flow export to define the export parameters for a flow.

**Note** Each flow exporter supports only one destination. If you want to export the data to multiple destinations, you must configure multiple flow exporters and assign them to the flow monitor.

You can export to a destination using IPv4 address.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **flow exporter** *name*<br>**Example:**<br>`Switch(config)# flow exporter ExportTest` | Creates a flow exporter and enters flow exporter configuration mode. |
| **Step 3** | **description** *string*<br>**Example:**<br>`Switch(config-flow-exporter)# description ExportV9` | (Optional) Describes this flow record as a maximum 63-character string. |
| **Step 4** | **destination** {*ipv4-address*} [ **vrf** *vrf-name*]<br>**Example:**<br>`Switch(config-flow-exporter)# destination 192.0.2.1 (IPv4 destination)` | Sets the IPv4 destination address or hostname for this exporter. |
| **Step 5** | **dscp** *value*<br>**Example:**<br>`Switch(config-flow-exporter)# dscp 0` | (Optional) Specifies the differentiated services codepoint value. The range is from 0 to 63. The default is 0. |
| **Step 6** | **source** { *source type* \|}<br>**Example:**<br>`Switch(config-flow-exporter)# source gigabitEthernet1/0/1` | (Optional) Specifies the interface to use to reach the NetFlow collector at the configured destination. The following interfaces can be configured as source:<br>\ |
| **Step 7** | **transport udp** *number*<br>**Example:**<br>`Switch(config-flow-exporter)# transport udp 200` | (Optional) Specifies the UDP port to use to reach the NetFlow collector. The range is from 1 to 65536 |
| **Step 8** | **ttl** *seconds*<br>**Example:**<br>`Switch(config-flow-exporter)# ttl 210` | (Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. The range is from 1 to 255 seconds. The default is 255. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | **export-protocol** {**netflow-v9**}<br>**Example:**<br>`Switch(config-flow-exporter)# export-protocol netflow-v9` | Specifies the version of the NetFlow export protocol used by the exporter. |
| **Step 10** | **end**<br>**Example:**<br>`Switch(config-flow-record)# end` | Returns to privileged EXEC mode. |
| **Step 11** | **show flow exporter** [**name** *record-name*]<br>**Example:**<br>`Switch# show flow exporter ExportTest` | (Optional) Displays information about NetFlow flow exporters. |
| **Step 12** | **copy running-config startup-config**<br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### What to do next

Define a flow monitor based on the flow record and flow exporter.

# Creating a Flow Monitor

Perform this required task to create a customized flow monitor.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. These record formats can be a user-defined format. An advanced user can create a customized format using the **flow record** command.

### Before you begin

If you want to use a customized record, you must create the customized record before you can perform this task. If you want to add a flow exporter to the flow monitor for data export, you must create the exporter before you can complete this task.

**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 on the flow monitor.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **flow monitor** *monitor-name*<br>**Example:**<br>`Switch(config)# flow monitor FLOW-MONITOR-1` | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode.<br>• This command also allows you to modify an existing flow monitor. |
| **Step 4** | **description** *description*<br>**Example:**<br>`Switch(config-flow-monitor)# description Used for basic ipv4 traffic analysis` | (Optional) Creates a description for the flow monitor. |
| **Step 5** | **record** {*record-name*}<br>**Example:**<br>`Switch(config-flow-monitor)# record FLOW-RECORD-1` | Specifies the record for the flow monitor. |
| **Step 6** | **cache** {**entries** *number* \| **timeout** {**active** \| **inactive** \| **update**} *seconds* \| { **normal** } | **timeout active** *seconds*—Configure the active flow timeout. This defines the granularity of the traffic analysis. The range is from 30 to 604800 seconds. The default is 1800. Typical values are 60 or 300 seconds. See the Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters document for recommended values. |
| **Step 7** | Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor. | — |
| **Step 8** | **exporter** *exporter-name*<br>**Example:**<br>`Switch(config-flow-monitor)# exporter EXPORTER-1` | (Optional) Specifies the name of an exporter that was created previously. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | **end**<br>**Example:**<br>`Switch(config-flow-monitor)# end` | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |
| **Step 10** | **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** \| **record** \| **table**} ]]]<br>**Example:**<br>`Switch# show flow monitor FLOW-MONITOR-2 cache` | (Optional) Displays the status for a Flexible NetFlow flow monitor. |
| **Step 11** | **show running-config flow monitor** *monitor-name*<br>**Example:**<br>`Switch# show running-config flow monitor FLOW_MONITOR-1` | (Optional) Displays the configuration of the specified flow monitor. |
| **Step 12** | **copy running-config startup-config**<br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Creating a Sampler

You can create a sampler to define the NetFlow sampling rate for a flow.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | **sampler** *name*<br>**Example:**<br>`Switch(config)# sampler SampleTest` | Creates a sampler and enters flow sampler configuration mode. |
| **Step 3** | **description** *string*<br>**Example:** | (Optional) Describes this flow record as a maximum 63-character string. |

| | Command or Action | Purpose |
|---|---|---|
| | `Switch(config-flow-sampler)# description samples` | |
| **Step 4** | **mode** {**deterministic** {*m* - *n*} \| **random** {*m* - *n*}}<br>**Example:**<br>`Switch(config-flow-sampler)# mode random 1 out-of 1022` | Defines the random sample mode.<br>You can configure either a random or deterministic sampler to an interface. Select *m* packets out of an *n* packet window. The window size to select packets from ranges from 32 to 1022.<br>Note the following when configuring a sampler to an interface:<br>• When you attach a monitor using deterministic sampler (for example, s1), every attachment with same sampler s1 uses one new free sampler from the switch (hardware) out of 4 available samplers. Therefore, beyond 4 attachments, you are not allowed to attach a monitor with any sampler.<br>• In contrast, when you attach a monitor using random sampler (for example-again, s1), only the first attachment uses a new sampler from the switch (hardware). The rest of all attachments using the same sampler s1, share the same sampler.<br>• Due to this behavior, when using a deterministic sampler, you can always make sure the correct number of flows are sampled by comparing the sampling rate and what the switch sends. If the same random sampler is used with multiple interfaces, flows from an interface can always be sampled, and the flows from other interfaces could be always skipped. |
| **Step 5** | **end**<br>**Example:**<br>`Switch(config-flow-sampler)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show sampler** [*name*]<br>**Example:**<br>`Switch show sample SampleTest` | (Optional) Displays information about NetFlow samplers. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **copy running-config startup-config**<br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### What to do next

Apply the flow monitor to a source interface or a VLAN.

# Applying a Flow to an Interface

You can apply a flow monitor and an optional sampler to an interface.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | **interface** *type*<br>**Example:**<br>`Switch(config)# interface GigabitEthernet1/0/1` | Enters interface configuration mode and configures an interface.<br>You cannot attach a NetFlow monitor to a port channel interface. If both service module interfaces are part of an EtherChannel, you should attach the monitor to both physical interfaces. |
| **Step 3** | {**ip flow monitor** \| **ipv6 flow monitor**}*name* [\| **sampler** *name*] {**input**}<br>**Example:**<br>`Switch(config-if)# ip flow monitor MonitorTest input` | Associate an IPv4 or an IPv6 flow monitor, and an optional sampler to the interface for input packets.<br>To monitor datalink L2 traffic flows, you would use **datalink flow monitor** *name* **sampler** *sampler-name* {**input**} interface command. This specific command associates a datalink L2 flow monitor and required sampler to the interface for input packets. When a datalink flow monitor is assigned to an interface or VLAN record, it only creates flows for non-IPv6 or non-IPv4 traffic. |
| **Step 4** | **end**<br>**Example:** | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Switch(config-flow-monitor)#  end` | |
| **Step 5** | **show flow interface** [*interface-type number*]<br>**Example:**<br>`Switch# show flow interface` | (Optional) Displays information about NetFlow on an interface. |
| **Step 6** | **copy running-config startup-config**<br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring NetFlow on SVI

You can apply a flow monitor and an optional sampler to a SVI.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | **interface vlan** *vlan-id*<br>**Example:**<br>`Switch(config)# interface vlan 30` | Specifies the SVI for the configuration. |
| **Step 3** | **ip flow monitor** *monitor name* [**sampler** *sampler name*] {**input** \| **output**}<br>**Example:**<br>`Switch(config-if)# ip flow monitor MonitorTest input` | Associates a flow monitor and an optional sampler to the SVI for input packets. |
| **Step 4** | **copy running-config startup-config**<br>**Example:**<br>`Switch# copy running-config` | (Optional) Saves your entries in the configuration file. |

| | Command or Action | Purpose |
|---|---|---|
| | `startup-config` | |

# Configuring Layer 2 NetFlow

You can define Layer 2 keys in Flexible NetFlow records that you can use to capture flows in Layer 2 interfaces.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | **flow record** *name*<br>**Example:**<br>`Switch(config)# flow record L2_record`<br>`Switch(config-flow-record)#` | Enters flow record configuration mode. |
| **Step 3** | **match datalink** {**ethertype** \| **mac** {**destination** {**address input**} \| **source** {**address input**}}}<br>**Example:**<br>`Switch(config-flow-record)# match datalink mac source address input`<br>`Switch(config-flow-record)# match datalink mac destination address input` | Specifies the Layer 2 attribute as a key. In this example, the keys are the source and destination MAC addresses from the packet at input.<br>**Note** When a datalink flow monitor is assigned to an interface or VLAN record, it only creates flows for non-IPv4 or non-IPv6 traffic. |
| **Step 4** | **end**<br>**Example:**<br>`Switch(config-flow-record)# end` | Returns to privileged EXEC mode. |
| **Step 5** | **show flow record** [*name*]<br>**Example:**<br>`Switch# show flow record` | (Optional) Displays information about NetFlow on an interface. |
| **Step 6** | **copy running-config startup-config**<br>**Example:** | (Optional) Saves your entries in the configuration file. |

| | Command or Action | Purpose |
|---|---|---|
| | `Switch# copy running-config startup-config` | |

# Monitoring Flexible NetFlow

The commands in the following table can be used to monitor Flexible NetFlow.

***Table 2: Flexible NetFlow Monitoring Commands***

| Command | Purpose |
|---|---|
| **show flow exporter** [**broker** \| **export-ids** \| **name** \| *name* \| **statistics** \| **templates**] | Displays information about NetFlow flow exporters and statistics. |
| **show flow exporter** [ **name** *exporter-name*] | Displays information about NetFlow flow exporters and statistics. |
| **show flow interface** | Displays information about NetFlow interfaces. |
| **show flow monitor** [ **name** *monitor-name*] | Displays information about NetFlow flow monitors and statistics. |
| **show flow monitor statistics** | Displays the statistics for the flow monitor |
| **show flow monitor***monitor-name* **cache format** {**table** \| **record** \| **csv**} | Displays the contents of the cache for the flow monitor, in the format specified. |
| **show flow record** [ **name** *record-name*] | Displays information about NetFlow flow records. |
| **show sampler** [**broker** \| **name** \| *name*] | Displays information about NetFlow samplers. |

# Configuration Examples for Flexible NetFlow

## Example: Configuring a Flow

This example shows how to create a flow and apply it to an interface:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# flow export export1
Switch(config-flow-exporter)# destination 10.0.101.254
Switch(config-flow-exporter)# transport udp 2055
Switch(config-flow-exporter)# exit
Switch(config)# flow record record1
Switch(config-flow-record)# match ipv4 source address
```

```
Switch(config-flow-record)# match ipv4 destination address
Switch(config-flow-record)# match ipv4 protocol
Switch(config-flow-record)# match transport source-port
Switch(config-flow-record)# match transport destination-port

Switch(config-flow-record)# collect counter byte long
Switch(config-flow-record)# collect counter packet long
Switch(config-flow-record)# collect timestamp sys-uptime first
Switch(config-flow-record)# collect timestamp sys-uptime last
Switch(config-flow-record)# exit
Switch(config)# flow monitor monitor1
Switch(config-flow-monitor)# record record1
Switch(config-flow-monitor)# exporter export1
Switch(config-flow-monitor)# exit
Switch(config)# interface tenGigabitEthernet 1/0/1
Switch(config-if)# ip flow monitor monitor1 input
Switch(config-if)# end
```

# Additional References for NetFlow

### Related Documents

| Related Topic | Document Title |
|---|---|
| Flexible NetFlow CLI Commands | NetFlow Command Reference |
| Catalyst 2960-X commands | Consolidated Platform Command Reference |
| Catalyst 2960-XR commands | Consolidated Platform Command Reference |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFC 3954 | Cisco Systems NetFlow Services Export Version 9 |

### MIBs

| MB | MIBs Link |
|---|---|
| | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br><br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br><br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

# Feature Information for Flexible NetFlow

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 3: Feature Information for Flexible NetFlow*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Flexible NetFlow | Cisco IOS Release 15.2(5)E1 | NetFlow is a Cisco IOS technology that provides statistics on packets flowing through the router. NetFlow is the standard for acquiring IP operational data from IP networks. NetFlow provides data to enable network and security monitoring, network planning, traffic analysis, and IP accounting.<br><br>In Cisco IOS Release 15.2(5)E1, this feature was introduced on Cisco Catalyst 2960-X Series Switches and Cisco Catalyst 2960-XR Series Switches. |
| Flexible NetFlow Lite | Cisco IOS Release 15.0(2)EX | In Cisco IOS Release 15.0(2)EX, this feature was introduced on Cisco Catalyst 2960-X Series Switches. |