Configuring NetFlow Lite

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

Prerequisites for NetFlow Lite

The following two targets for attaching a NetFlow Lite monitor are supported:

- 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.

Restrictions for NetFlow Lite

The following are restrictions for NetFlow Lite:

- 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 port-based monitor to an interface at the same time on the switch. A 48-port switch 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 switch 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:
  - Only sampled NetFlow is supported.
  - For both port and VLANS, a total of only 4 samplers (random or deterministic) are supported on the switch.
  - 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.
  - You must associate a sampler with a monitor while attaching it to an interface. Otherwise, the command will be rejected. Use the **ip flow monitor** *monitor_name* sampler s*ampler_name* **input** interface configuration command to perform this task.
  - 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 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 switch 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.

- Network flows and statistics are collected at the line rate.
- ACL-based NetFlow is not supported.
- Only NetFlow Version 9 is supported for Flexible NetFlow exporter using the *export-protocol* command option. If you configure NetFlow Version 5, this version will be accepted, but the NetFlow Version 5 export functionality is neither currently available nor supported.
- The switch supports homogeneous stacking, but does not support mixed stacking.

Information About NetFlow Lite

NetFlow Lite Overview

NetFlow Lite 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 NetFlow Lite feature that enables enhanced network anomalies and security detection. NetFlow Lite 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 NetFlow Lite cache.

You can export the data that NetFlow Lite gathers for your flow by using an exporter and export this data to a remote system such as a NetFlow Lite collector. The NetFlow Lite 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 NetFlow Lite cache information.

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

Related Topics

Creating a Flow Record, on page 11
Example: Configuring a Flow, on page 23

NetFlow Predefined Records

Flexible NetFlow includes several predefined records that you can use to start monitoring traffic in your network. The predefined records are available to help you quickly deploy Flexible NetFlow and are easier to use than user-defined flow records. You can choose from a list of already defined records that may meet the needs for network monitoring. As Flexible NetFlow evolves, popular user-defined flow records will be made available as predefined records to make them easier to implement.

The predefined records ensure backward compatibility with your existing NetFlow collector configurations for the data that is exported. Each of the predefined records has a unique combination of key and nonkey fields that offer you the built-in ability to monitor various types of traffic in your network without customizing Flexible NetFlow on your router.

Two of the predefined records (NetFlow original and NetFlow IPv4/IPv6 original output), which are functionally equivalent, emulate original (ingress) NetFlow and the Egress NetFlow Accounting feature in original NetFlow, respectively. Some of the other Flexible NetFlow predefined records are based on the aggregation cache schemes available in original NetFlow. The Flexible NetFlow predefined records that are based on the aggregation cache schemes available in original NetFlow do not perform aggregation. Instead each flow is tracked separately by the predefined records.

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.

NetFlow Lite Match Parameters

You can match these key fields for the flow record:

- IPv4 or IPv6 destination address
- Datalink fields (source and destination MAC address, and MAC ethertype (type of networking protocol)).
- Transport field source and destination ports to identify the type of application: ICMP, IGMP, or TCP traffic.

The following table describes NetFlow Lite match parameters. You must configure at least one of the following match parameters for the flow records.

Table 1: Match Parameters

Command	Purpose
match datalink {**ethertype** | **mac** {**destination address input** | **source address input**}}	Specifies a match to datalink or Layer 2 fields. The following command options are available: • **ethertype**—Matches to the ethertype of the packet. • **mac**—Matches the source or destination MAC address from packets at input. **Note** When a datalink flow monitor is assigned to an interface or VLAN, it only creates flows for non-IPv6 or non-IPv4 traffic.
match ipv4 {**destination** {**address**} | **protocol** | **source** {**address**} | **tos**}	Specifies a match to the IPv4 fields. The following command options are available: • **destination**—Matches to the IPv4 destination address-based fields. • **protocol**—Matches to the IPv4 protocols. • **source**—Matches to the IPv4 source address based fields. • **tos**—Matches to the IPv4 Type of Service fields.
match ipv6 {**destination** {**address**} | **flow-label** | **protocol** | **source** {**address**} | **traffic-class**}	Specifies a match to the IPv6 fields. The following command options are available: • **destination**—Matches to the IPv6 destination address-based fields. • **flow-label**—Matches to the IPv6 flow-label fields. • **protocol**—Matches to the IPv6 payload protocol fields. • **source**—Matches to the IPv6 source address based fields. • **traffic-class**—Matches to the IPv6 traffic class.
match transport {**destination-port** | **source-port**}	Specifies a match to the Transport Layer fields. The following command options are available: • **destination-port**—Matches to the transport destination port. • **source-port**—Matches to the transport source port.

Command	Purpose
	Specifies the use of SSID of the wireless network as a key field for a flow record.

NetFlow Lite Collect Parameters

You can collect these key fields in the flow record:

- The total number of bytes, flows or packets sent by the exporter (exporter) or the number of bytes or packets in a 64-bit counter (long).
- The timestamp based on system uptime from the time the first packet was sent or from the time the most recent (last) packet was seen.
- The SNMP index of the input interface. The interface for traffic entering the service module is based on the switch forwarding cache. This field is typically used in conjunction with datalink, IPv4, and IPv6 addresses, and provides the actual first-hop interface for directly connected hosts.
  - A value of 0 means that interface information is not available in the cache.
  - Some NetFlow collectors require this information in the flow record.

The following table describes NetFlow Lite collect parameters.

Table 2: Collect Parameters

Command	Purpose
collect counter {**bytes** {**long** | **permanent** } | **packets** { **long** | **permanent**}}	Collects the counter fields total bytes and total packets.
collect flow {**sampler**}	Collects the flow sampler identifier (ID).
collect interface {**input**}	Collects the fields from the input interface.
collect timestamp sys-uptime {**first** | **last**}	Collects the fields for the time the first packet was seen or the time the most recent packet was last seen (in milliseconds).
collect transport tcp flags	Collects the following transport TCP flags: • **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

Command	Purpose
	Collects the MAC addresses of the access points that the wireless client is associated with.

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.

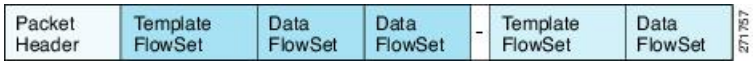
NetFlow Data Export Format Version 9

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.

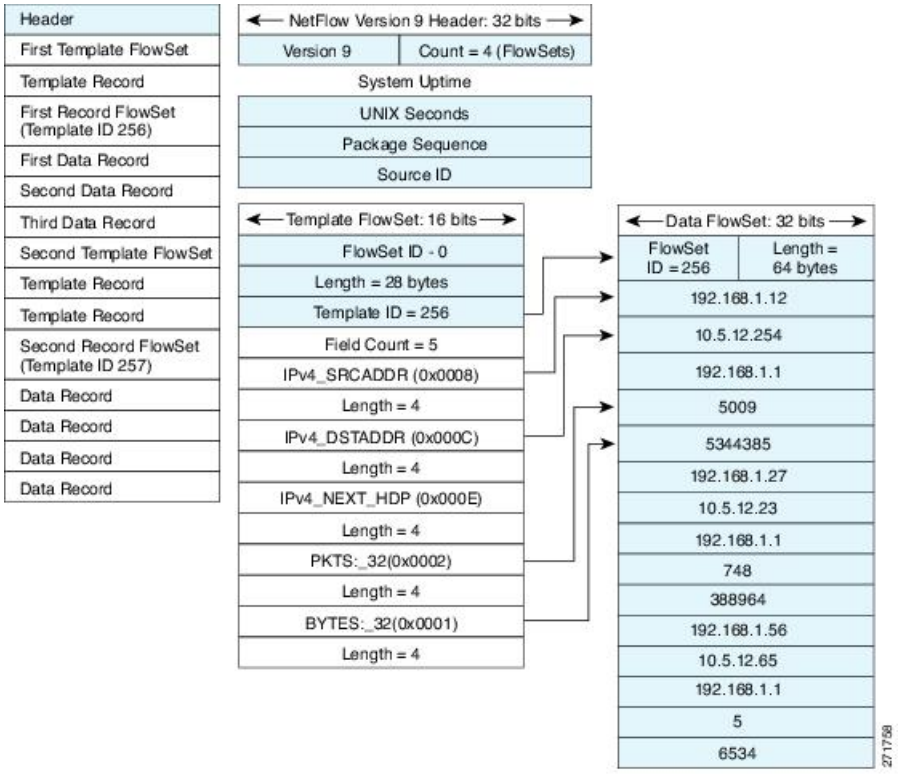
The Version 9 export format consists of a packet header followed by one or more template flow or data flow sets. A template flow set provides a description of the fields that will be present in future data flow sets. These data flow sets may occur later within the same export packet or in subsequent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

Figure 1: 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 2: Detailed Example of the NetFlow Version 9 Export Format



For more information on the Version 9 export format, refer to the white paper titled Cisco IOS NetFlow Version 9 Flow-Record Format, available at this URL: http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper09186a00800a3db9.shtml.

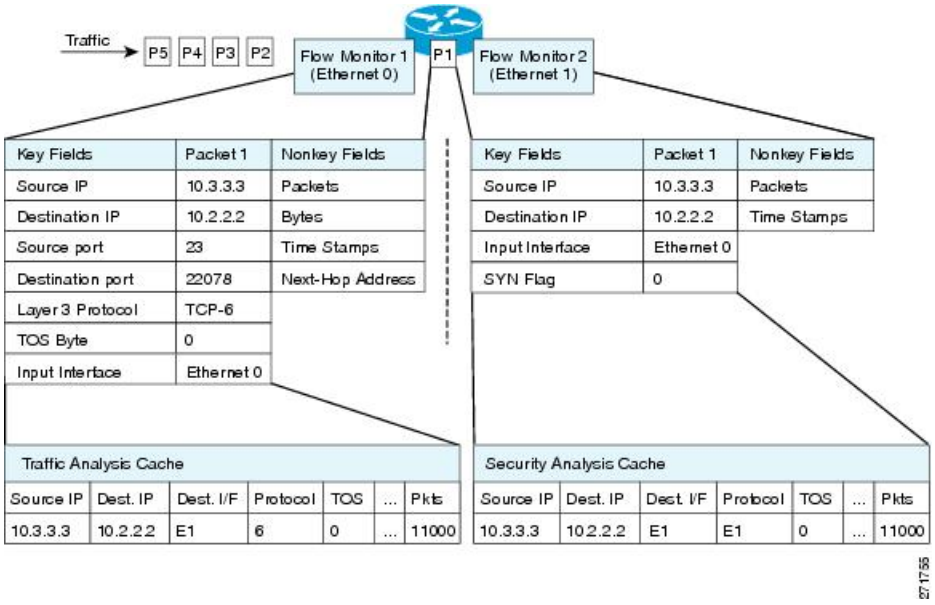
Flow Monitors

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.

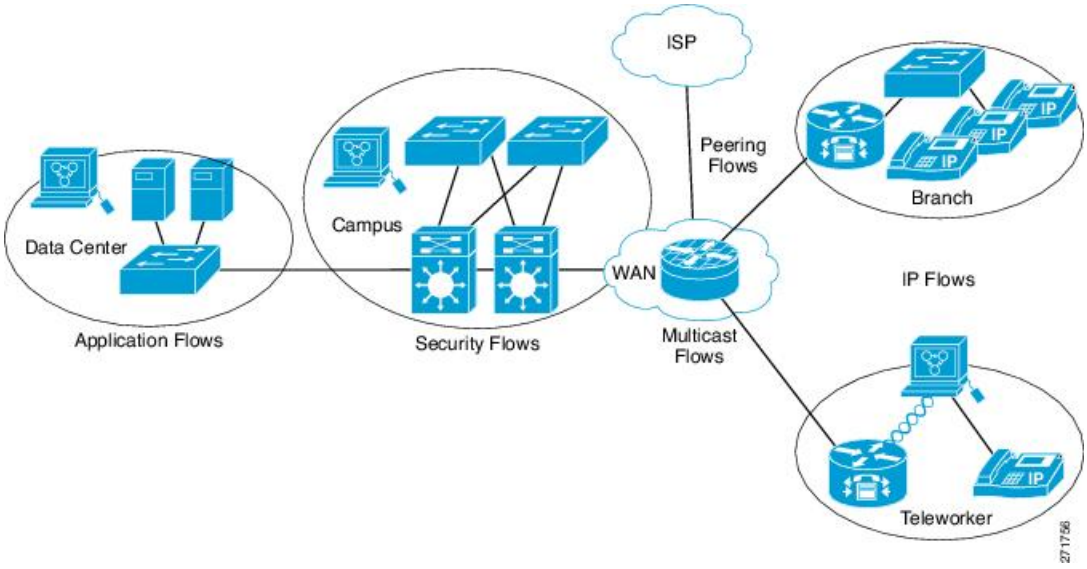
Flexible NetFlow can be used to perform different types of analysis on the same traffic. In the figure below, packet 1 is analyzed using a record designed for standard traffic analysis on the input interface and a record designed for security analysis on the output interface.

Figure 3: Example of Using Two Flow Monitors to Analyze the Same Traffic



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

Figure 4: 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 NetFlow Lite 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.

Default Settings

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

Table 3: Default NetFlow Lite Settings

Setting	Default
Flow active timeout	1800 seconds **Note** The default value for this setting may be too high for your specific NetFlow Lite 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 bits

How to Configure NetFlow Lite

To configure NetFlow Lite, 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

You can create a flow record and add keys to match on and fields to collect in the flow.

SUMMARY STEPS

1. **configure terminal**
2. **flow record** *name*
3. **description** *string*
4. **match** *type*
5. **collect** *type*
6. **end**
7. **show flow record** [**name** *record-name*]
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchDevice# configure terminal`	Enters the global configuration mode.

Step 2	**flow record** *name*
	Example:
	`SwitchDevice(config)# flow record test`
	`SwitchDevice(config-flow-record)#`
		Creates a flow record and enters flow record configuration mode.

Step 3	**description** *string* **Example:** `SwitchDevice(config-flow-record)# description Ipv4Flow`	(Optional) Describes this flow record as a maximum 63-character string.

Step 4	**match** *type*
	Example:
	`SwitchDevice(config-flow-record)# match ipv4 source address`
	`SwitchDevice(config-flow-record)# match ipv4 destination address`
	`SwitchDevice(config-flow-record)# match flow direction`
		Specifies a match key.

	Command or Action	Purpose

Step 5	**collect** *type*
	Example:
	`SwitchDevice(config-flow-record)# collect counter bytes layer2 long`
	`SwitchDevice(config-flow-record)# collect counter bytes long`
	`SwitchDevice(config-flow-record)# collect timestamp absolute first`
	`SwitchDevice(config-flow-record)# collect transport tcp flags`
	`SwitchDevice(config-flow-record)# collect interface output`
		Specifies the collection field.
		Note When a flow monitor has the **collect interface output** as the collect field in the flow record, then the output interface is detected based on the destination address in the switch. Hence, for the different flow monitors, the following are required to be configured:
		• For ipv4 flow monitor, configure "**match ip destination address**"
		• For ipv6 flow monitor, configure "**match ipv6 destination address**"
		• For datalink flow monitor, configure "**match datalink mac output**"
		The **collect interface output** field will return a value of **NULL** when a flow gets created for any of the following addresses:
		• L3 broadcast
		• L2 broadcast
		• L3 Multicast
		• L2 Multicast
		• L2 unknown destination.

Step 6	**end** **Example:** `SwitchDevice(config-flow-record)# end`	Returns to privileged EXEC mode.
Step 7	**show flow record** [**name** *record-name*] **Example:** `SwitchDevice show flow record test`	(Optional) Displays information about NetFlow flow records.
Step 8	**copy running-config startup-config** **Example:** `SwitchDevice# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

Define an optional flow exporter by specifying the export format, protocol, destination, and other parameters.

Related Topics

Flow Records, on page 3
Example: Configuring a Flow, on page 23

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.

SUMMARY STEPS

1. **configure terminal**
2. **flow exporter** *name*
3. **description** *string*
4. **destination** {*ipv4-address*} [**vrf** *vrf-name*]
5. **dscp** *value*
6. **source** { *source type* }
7. **transport udp** *number*
8. **ttl** *seconds*
9. **export-protocol** {**netflow-v9**}
10. **end**
11. **show flow exporter** [**name** *record-name*]
12. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchDevice# configure terminal`	Enters the global configuration mode.
Step 2	**flow exporter** *name* **Example:** `SwitchDevice(config)# flow exporter ExportTest`	Creates a flow exporter and enters flow exporter configuration mode.

	Command or Action	Purpose
Step 3	**description** *string* **Example:** `SwitchDevice(config-flow-exporter)# description ExportV9`	(Optional) Describes this flow record as a maximum 63-character string.
Step 4	**destination** {*ipv4-address*} [**vrf** *vrf-name*] **Example:** `SwitchDevice(config-flow-exporter)# destination 192.0.2.1 (IPv4 destination)`	Sets the IPv4 destination address or hostname for this exporter.
Step 5	**dscp** *value* **Example:** `SwitchDevice(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* } **Example:** `SwitchDevice(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:
Step 7	**transport udp** *number* **Example:** `SwitchDevice(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* **Example:** `SwitchDevice(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.
Step 9	**export-protocol** {**netflow-v9**} **Example:** `SwitchDevice(config-flow-exporter)# export-protocol netflow-v9`	Specifies the version of the NetFlow export protocol used by the exporter.
Step 10	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`SwitchDevice(config-flow-record)# end`	
Step 11	**show flow exporter** [**name** *record-name*] **Example:** `SwitchDevice show flow exporter ExportTest`	(Optional) Displays information about NetFlow flow exporters.
Step 12	**copy running-config startup-config** **Example:** `SwitchDevice# 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.

Related Topics

Exporters
Example: Configuring a Flow, on page 23

Creating a Flow Monitor

You can create a flow monitor and associate it with a flow record and a flow exporter.

SUMMARY STEPS

1. **configure terminal**
2. **flow monitor** *name*
3. **description** *string*
4. **exporter** *name*
5. **record** *name*
6. **cache** { **timeout** {**active** | **inactive**} *seconds* | **type normal** }
7. **end**
8. **show flow monitor** [**name** *record-name*]
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`SwitchDevice# configure terminal`	

Step 2	**flow monitor** *name*
	Example:
	`SwitchDevice(config)# flow monitor MonitorTest`
	`SwitchDevice (config-flow-monitor)#`
		Creates a flow monitor and enters flow monitor configuration mode.

Step 3	**description** *string* **Example:** `SwitchDevice(config-flow-monitor)# description Ipv4Monitor`	(Optional) Describes this flow record as a maximum 63-character string.
Step 4	**exporter** *name* **Example:** `SwitchDevice(config-flow-monitor)# exporter ExportTest`	Associates a flow exporter with this flow monitor.
Step 5	**record** *name* **Example:** `SwitchDevice(config-flow-monitor)# record test`	Associates a flow record with the specified flow monitor.
Step 6	**cache** { **timeout** {**active** | **inactive**} *seconds* | **type normal** } **Example:** `SwitchDevice(config-flow-monitor)# cache timeout active 15000`	Associates a flow cache with the specified flow monitor.
Step 7	**end** **Example:** `SwitchDevice(config-flow-monitor)#  end`	Returns to privileged EXEC mode.
Step 8	**show flow monitor** [**name** *record-name*] **Example:** `SwitchDevice show flow monitor name MonitorTest`	(Optional) Displays information about NetFlow flow monitors.

	Command or Action	Purpose
Step 9	**copy running-config startup-config** **Example:** `SwitchDevice# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

Apply the flow monitor to a Layer 2 interface, Layer 3 interface, or VLAN.

Related Topics

Monitors
Example: Configuring a Flow, on page 23

Creating a Sampler

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

SUMMARY STEPS

1. **configure terminal**
2. **sampler** *name*
3. **description** *string*
4. **mode** { **deterministic** { *m* - *n* } | **random** { *m* - *n* }}
5. **end**
6. **show sampler** [*name*]
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchDevice# configure terminal`	Enters the global configuration mode.

Step 2	**sampler** *name*
	Example:
	`SwitchDevice(config)# sampler SampleTest`
	`SwitchDevice(config-flow-sampler)#`
		Creates a sampler and enters flow sampler configuration mode.

Step 3	**description** *string* **Example:**	(Optional) Describes this flow record as a maximum 63-character string.

	Command or Action	Purpose
	`SwitchDevice(config-flow-sampler)# description samples`	
Step 4	**mode** { **deterministic** { *m* - *n* } | **random** { *m* - *n* }} **Example:** `SwitchDevice(config-flow-sampler)# mode random 1 out-of 1022`	Defines the random sample mode. 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. Note the following when configuring a sampler to an interface: • 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. • 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. 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** **Example:** `SwitchDevice(config-flow-sampler)# end`	Returns to privileged EXEC mode.
Step 6	**show sampler** [*name*] **Example:** `SwitchDevice show sample SampleTest`	(Optional) Displays information about NetFlow samplers.
Step 7	**copy running-config startup-config** **Example:** `SwitchDevice# copy running-config`	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`startup-config`	

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type*
3. {**ip flow monitor** | **ipv6 flow monitor**}*name* [|**sampler** *name*] { **input** |**output** }
4. **end**
5. **show flow interface** [*interface-type number*]
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchDevice# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *type* **Example:** `SwitchDevice(config)# interface GigabitEthernet1/0/1`	Enters interface configuration mode and configures an interface. Command parameters for the interface configuration include: 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** |**output** } **Example:** `SwitchDevice(config-if)# ip flow monitor MonitorTest input`	Associate an IPv4 or an IPv6 flow monitor, and an optional sampler to the interface for input or output packets. 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.

	Command or Action	Purpose
		Note Whenever you assign a flow monitor to an interface, you must configure a sampler. If the sampler is missing, you will receive an error message.
Step 4	**end** **Example:** `SwitchDevice(config-flow-monitor)# end`	Returns to privileged EXEC mode.
Step 5	**show flow interface** [*interface-type number*] **Example:** `SwitchDevice# show flow interface`	(Optional) Displays information about NetFlow on an interface.
Step 6	**copy running-config startup-config** **Example:** `SwitchDevice# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring a Bridged NetFlow on a VLAN

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

SUMMARY STEPS

1. **configure terminal**
2. **vlan** [**configuration**] *vlan-id*
3. **interface** {**vlan**} *vlan-id*
4. **ip flow monitor** *monitor name* [**sampler** *sampler name*] {**input** |**output**}
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchDevice# configure terminal`	Enters the global configuration mode.
Step 2	**vlan** [**configuration**] *vlan-id* **Example:**	Enters VLAN or VLAN configuration mode.

	Command or Action	Purpose
	`SwitchDevice(config)# vlan configuration 30` `SwitchDevice(config-vlan-config)#`	
Step 3	**interface** {**vlan**} *vlan-id* **Example:** `SwitchDevice(config)# interface vlan 30`	Specifies the SVI for the configuration.
Step 4	**ip flow monitor** *monitor name* [**sampler** *sampler name*] {**input** |**output**} **Example:** `SwitchDevice(config-vlan-config)# ip flow monitor MonitorTest input`	Associates a flow monitor and an optional sampler to the VLAN for input or output packets.
Step 5	**copy running-config startup-config** **Example:** `SwitchDevice# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Layer 2 NetFlow

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

SUMMARY STEPS

1. **configure terminal**
2. **flow record** *name*
3. **match datalink** { **ethertype** | **mac** { **destination** { **address input** } | **source** { **address input** } } }
4. **match** { **ipv4** {**destination** | **protocol** | **source** | **tos** } | **ipv6** {**destination** | **flow-label**| **protocol**| **source**| **traffic-class** } | **transport** {**destination-port** | **source-port**} }
5. **end**
6. **show flow record** [*name*]
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`SwitchDevice# configure terminal`	

Step 2	**flow record** *name*
	Example:
	`SwitchDevice(config)# flow record L2_record`
	`SwitchDevice(config-flow-record)#`
		Enters flow record configuration mode.

Step 3	**match datalink** { **ethertype** | **mac** { **destination** { **address input** } | **source** { **address input** } } }
	Example:
	`SwitchDevice(config-flow-record)# match datalink mac source address input`
	`SwitchDevice(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.
		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	**match** { **ipv4** {**destination** | **protocol** | **source** | **tos** } | **ipv6** {**destination** | **flow-label**| **protocol**| **source**| **traffic-class** } | **transport** {**destination-port** | **source-port**} }
	Example:
	`SwitchDevice(config-flow-record)# match ipv4 protocol`
	`SwitchDevice(config-flow-record)# match ipv4 tos`
		Specifies additional Layer 2 attributes as a key. In this example, the keys are IPv4 protocol and ToS.

Step 5	**end** **Example:** `SwitchDevice(config-flow-record)#  end`	Returns to privileged EXEC mode.
Step 6	**show flow record** [*name*] **Example:** `SwitchDevice# show flow record`	(Optional) Displays information about NetFlow on an interface.
Step 7	**copy running-config startup-config** **Example:** `SwitchDevice# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Monitoring Flexible NetFlow

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

Table 4: 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** *exporter-name*]	Displays information about NetFlow flow monitors and statistics.
show flow monitor statistics	Displays the statistics for the flow monitor
show flow monitor 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 flow ssid	Displays NetFlow monitor installation status for a WLAN.
show sampler [**broker** | **name** | *name*]	Displays information about NetFlow samplers.
show wlan *wlan-name*	Displays the WLAN configured on the device.

Configuration Examples for NetFlow Lite

Example: Configuring a Flow

Note When configuring a flow, you need to have the protocol, source port, destination port, first and last timestamps, and packet and bytes counters defined in the flow record. Otherwise, you will get the following error message: "Warning: Cannot set protocol distribution with this Flow Record. Require protocol, source and destination ports, first and last timestamps and packet and bytes counters."

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

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

```
SwitchDevice(config)# flow exporter export1
SwitchDevice(config-flow-exporter)# destination 10.0.101.254
SwitchDevice(config-flow-exporter)# transport udp 2055
SwitchDevice(config-flow-exporter)# template data timeout 60
SwitchDevice(config-flow-exporter)# exit
SwitchDevice(config)# flow record record1
SwitchDevice(config-flow-record)# match ipv4 source address
SwitchDevice(config-flow-record)# match ipv4 destination address
SwitchDevice(config-flow-record)# match ipv4 protocol
SwitchDevice(config-flow-record)# match transport source-port
SwitchDevice(config-flow-record)# match transport destination-port
SwitchDevice(config-flow-record)# collect counter bytes long
SwitchDevice(config-flow-record)# collect counter packets long
SwitchDevice(config-flow-record)# collect timestamp sys-uptime first
SwitchDevice(config-flow-record)# collect timestamp sys-uptime last
SwitchDevice(config-flow-record)# exit
SwitchDevice(config)# sampler SampleTest
SwitchDevice(config-sampler)# mode random 1 out-of 100
SwitchDevice(config-sampler)# exit
SwitchDevice(config)# flow monitor monitor1
SwitchDevice(config-flow-monitor)# cache timeout active 300
SwitchDevice(config-flow-monitor)# cache timeout inactive 120
SwitchDevice(config-flow-monitor)# record record1
SwitchDevice(config-flow-monitor)# exporter export1
SwitchDevice(config-flow-monitor)# exit
SwitchDevice(config)# interface GigabitEthernet1/0/1
SwitchDevice(config-if)# ip flow monitor monitor1 sampler SampleTest input
SwitchDevice(config-if)# end
```

Related Topics

Creating a Flow Record, on page 11
Flow Records, on page 3
Creating a Flow Exporter, on page 13
Exporters
Creating a Flow Monitor, on page 15
Monitors
Creating a Sampler
Samplers