



Configuring Flexible NetFlow

- [Finding Feature Information, on page 1](#)
- [Prerequisites for Flexible NetFlow, on page 1](#)
- [Restrictions for Flexible NetFlow, on page 2](#)
- [Information About Flexible Netflow, on page 2](#)
- [How to Configure Flexible Netflow, on page 12](#)
- [Monitoring Flexible NetFlow, on page 22](#)
- [Configuration Examples for Flexible NetFlow, on page 23](#)
- [Additional References for NetFlow, on page 24](#)

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 at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <https://cfnng.cisco.com/>. An account on Cisco.com is not required.

Prerequisites for Flexible NetFlow

- You are familiar with the Flexible NetFlow key fields as they are defined in the following commands:
 - **match flow**
 - **match interface**
 - **match {ipv4 | ipv6}**
 - **match routing**
 - **match transport**
- You are familiar with the Flexible NetFlow nonkey fields as they are defined in the following commands:
 - **collect counter**
 - **collect flow**
 - **collect interface**

- `collect {ipv4 | ipv6}`
- `collect routing`
- `collect timestamp sys-uptime`
- `collect transport`

- The networking device must be running a Cisco release that supports Flexible NetFlow.

IPv4 Traffic

- The networking device must be configured for IPv4 routing.
- 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.

IPv6 Traffic

- The networking device must be configured for IPv6 routing.
- 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 IPv6 or distributed Cisco Express Forwarding.

Restrictions for Flexible NetFlow

The following are restrictions for Flexible NetFlow:

- Microflow policing feature shares the NetFlow hardware resource with FNF.
- Only one flow monitor per interface and per direction is supported .
- The switch supports up to 16 flow monitors.
-
- For an IPv6 flow monitor, Source Group Tag (SGT) and Destination Group Tag (DGT) fields cannot co-exist with MAC address fields

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.

Starting with the Cisco IOS XE 16.12.1 release, Source Group Tag (SGT) and Destination Group Tag (DGT) fields over Flexible NetFlow are supported for IPv6 traffic.

Original NetFlow and Benefits of Flexible NetFlow

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

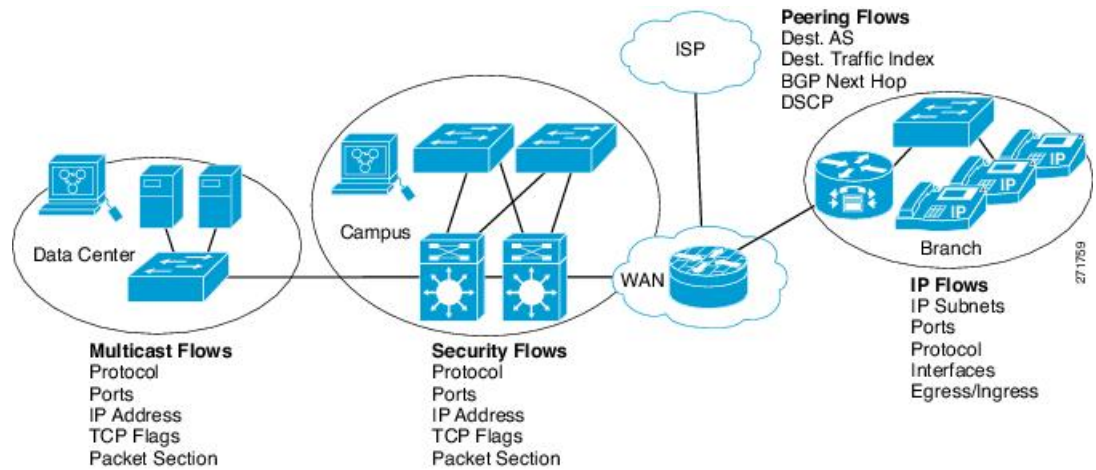
- High-capacity flow recognition, including scalability and aggregation of flow information.
- Enhanced flow infrastructure for security monitoring and dDoS detection and identification.
- New information from packets to adapt flow information to a particular service or operation in the network. The 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.

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.

Related Topics

- [Creating a Flow Record](#), on page 13
- [Example: Configuring a Flow](#), on page 23

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.

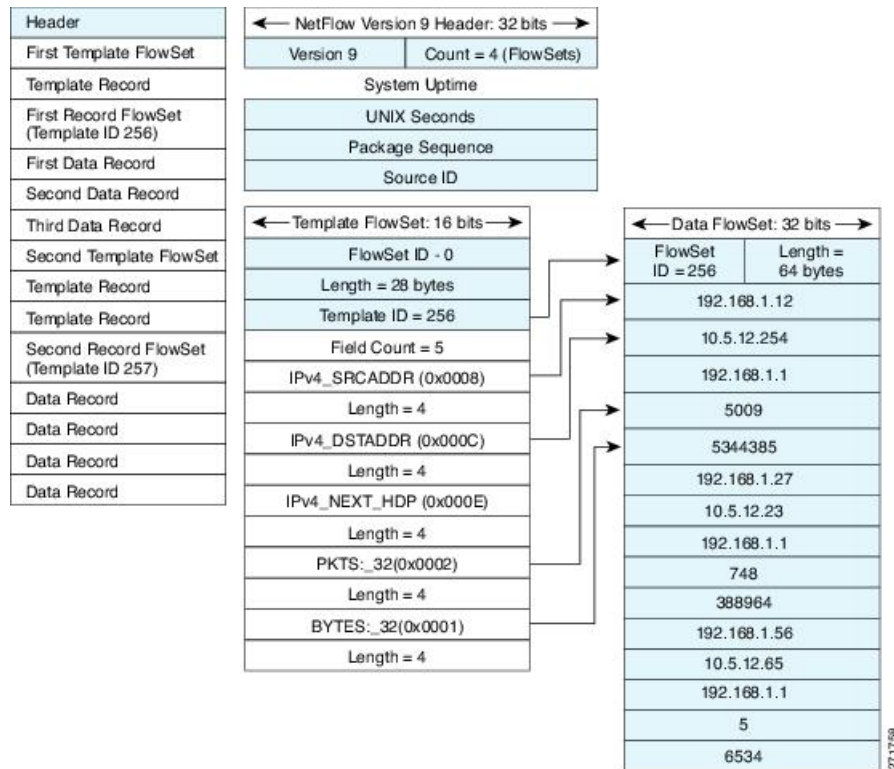
Figure 2: Version 9 Export Packet



271757

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



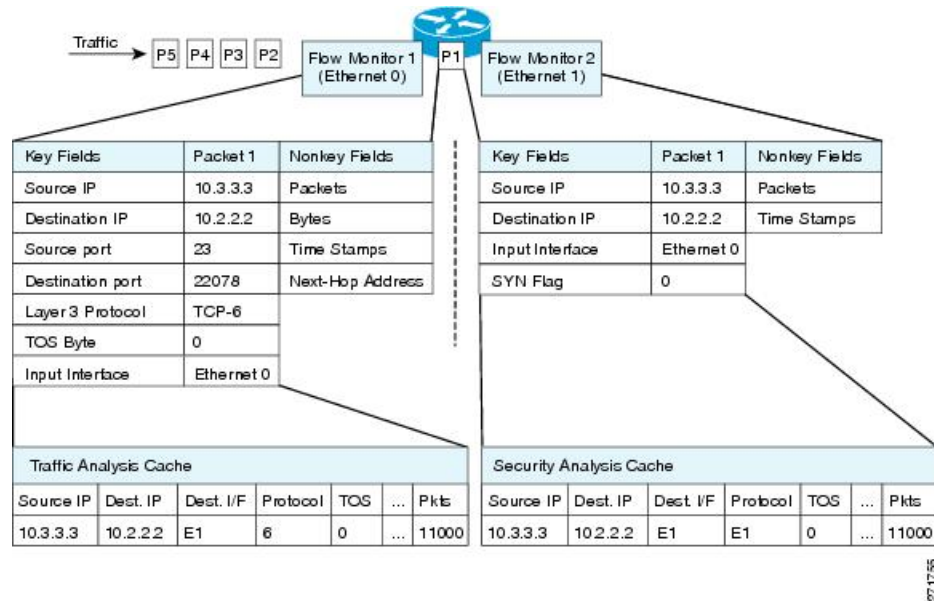
Flow Monitors

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.

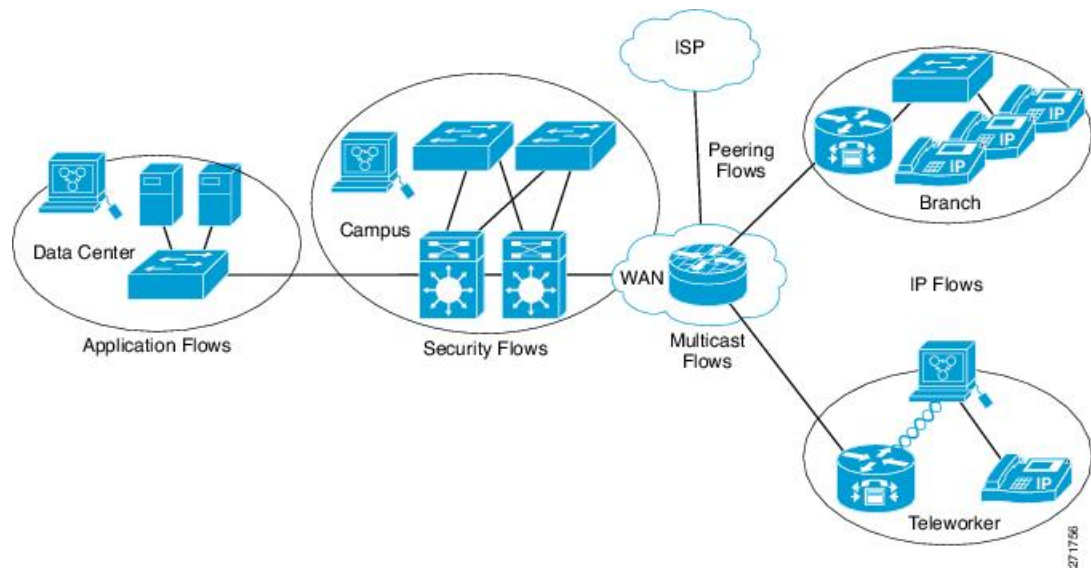
Flexible NetFlow can be used to perform different types of analysis on the same traffic. In the figure below, packet 1 is analyzed using a record designed for standard traffic analysis on the input interface and a record designed for security analysis on the output interface.

Figure 4: 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 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 tables provide a consolidated list of supported fields in Flexible NetFlow (FNF) for various traffic types and traffic direction.



Note If the packet has a VLAN field, then that length is not accounted for.

Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
Key or Collect Fields							
Interface input	Yes	—	Yes	—	Yes	—	If you apply a flow monitor in the input direction: <ul style="list-style-type: none"> • Use the match keyword and use the input interface as a key field. • Use the collect keyword and use the output interface as a collect field. This field will be present in the exported records but with a value of 0.

Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
Interface output	—	Yes	—	Yes	—	Yes	<p>If you apply a flow monitor in the output direction:</p> <ul style="list-style-type: none"> • Use the match keyword and use the output interface as a key field. • Use the collect keyword and use the input interface as a collect field. This field will be present in the exported records but with a value of 0.

Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
Key Fields							
Flow direction	Yes	Yes	Yes	Yes	Yes	Yes	
Ethertype	Yes	Yes	—	—	—	—	
VLAN input	Yes	—	Yes	—	Yes	—	Supported only for a switch port.
VLAN output	—	Yes	—	Yes	—	Yes	Supported only for a switch port.
dot1q VLAN input	Yes	—	Yes	—	Yes	—	Supported only for a switch port.
dot1q VLAN output	—	Yes	—	Yes	—	Yes	Supported only for a switch port.
dot1q priority	Yes	Yes	Yes	Yes	Yes	Yes	Supported only for a switch port.
MAC source address input	Yes	Yes	Yes	Yes	Yes	Yes	

Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
MAC source address output	—	—	—	—	—	—	
MAC destination address input	Yes	—	Yes	—	Yes	—	
MAC destination address output	—	Yes	—	Yes	—	Yes	
IPv4 version	—	—	Yes	Yes	Yes	Yes	
IPv4 TOS	—	—	Yes	Yes	Yes	Yes	
IPv4 protocol	—	—	Yes	Yes	Yes	Yes	Must use if any of src/dest port, ICMP code/type, IGMP type or TCP flags are used.
IPv4 TTL	—	—	Yes	Yes	Yes	Yes	
IPv4 source address	—	—	Yes	Yes	—	—	
IPv4 destination address	—	—	Yes	Yes	—	—	
ICMP IPv4 type	—	—	Yes	Yes	—	—	
ICMP IPv4 code	—	—	Yes	Yes	—	—	
IGMP type	—	—	Yes	Yes	—	—	
Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
Key Fields continued							

Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
IPv6 version	—	—	Yes	Yes	Yes	Yes	Same as IP version.
IPv6 protocol	—	—	Yes	Yes	Yes	Yes	Same as IP protocol. Must use if any of src/dest port, ICMP code/type, IGMP type or TCP flags are used.
IPv6 source address	—	—	—	—	Yes	Yes	
IPv6 destination address	—	—	—	—	Yes	Yes	
IPv6 traffic-class	—	—	Yes	Yes	Yes	Yes	Same as IP TOS.
IPv6 hop-limit	—	—	Yes	Yes	Yes	Yes	Same as IP TTL.
ICMP IPv6 type	—	—	—	—	Yes	Yes	
ICMP IPv6 code	—	—	—	—	Yes	Yes	
source-port	—	—	Yes	Yes	Yes	Yes	
dest-port	—	—	Yes	Yes	Yes	Yes	
Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
Collect Fields							

Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
Bytes long	Yes	Yes	Yes	Yes	Yes	Yes	Packet size = (Ethernet frame size including FCS - 18 bytes) Recommended: Avoid this field and use Bytes layer2 long.
Packets long	Yes	Yes	Yes	Yes	Yes	Yes	
Timestamp absolute first	Yes	Yes	Yes	Yes	Yes	Yes	
Timestamp absolute last	Yes	Yes	Yes	Yes	Yes	Yes	
TCP flags	Yes	Yes	Yes	Yes	Yes	Yes	Collects all flags.
Bytes layer2 long	Yes	Yes	Yes	Yes	Yes	Yes	

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
Flow timeout inactive	15 seconds

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 Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	flow record <i>record-name</i> Example: Device(config)# flow record FLOW-RECORD-1	Creates a flow record and enters Flexible NetFlow flow record configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow record.
Step 4	description <i>description</i> Example: Device(config-flow-record)# description Used for basic traffic analysis	(Optional) Creates a description for the flow record.
Step 5	match {ip ipv6} {destination source} address Example: 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.

	Command or Action	Purpose
Step 6	Repeat Step 5 as required to configure additional key fields for the record.	—
Step 7	<p>match flow cts {source destination} group-tag</p> <p>Example:</p> <pre>Device(config-flow-record)# match flow cts source group-tag</pre> <pre>Device(config-flow-record)# match flow cts destination group-tag</pre>	<p>Note This example configures the CTS source group tag and destination group tag as a key field for the record. For information about the other key fields available for the match ipv4/ipv6 command, and the other match commands that are available to configure key fields.</p> <p>Note</p> <ul style="list-style-type: none"> • Ingress: <ul style="list-style-type: none"> • In an incoming packet, if a header is present, SGT will reflect the same value as the header. If no value is present, it will show zero. • The DGT value will not depend on the ingress port SGACL configuration. • Egress: <ul style="list-style-type: none"> • If either propagate SGT or CTS is disabled on the egress interface, then SGT will be zero. • In an outgoing packet, if SGACL configuration that corresponds to the (SGT, DGT) exists, DGT will be non-zero. • If SGACL is disabled on the egress port/VLAN or if global SGACL enforcement is disabled, then DGT will be zero

	Command or Action	Purpose
Step 8	<ul style="list-style-type: none"> • collect counter {bytes [exported long] flows [exported] packets} [exported long] • or • collect timestamp sys-uptime {first last} <p>Example:</p> <pre>Device(config-flow-record)# collect counter bytes</pre>	<p>Configures the input interface as a nonkey field for the record.</p> <p>Note This example configures the input interface as a nonkey field for the record.</p>
Step 9	Repeat the above step as required to configure additional nonkey fields for the record.	—
Step 10	<p>end</p> <p>Example:</p> <pre>Device(config-flow-record)# end</pre>	Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode.
Step 11	<p>show flow record <i>record-name</i></p> <p>Example:</p> <pre>Device# show flow record FLOW_RECORD-1</pre>	(Optional) Displays the current status of the specified flow record.
Step 12	<p>show running-config flow record <i>record-name</i></p> <p>Example:</p> <pre>Device# show running-config flow record FLOW_RECORD-1</pre>	(Optional) Displays the configuration of the specified flow record.

Related Topics

[User-Defined Records](#), on page 5

[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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	flow exporter name Example: Switch(config)# flow exporter ExportTest	Creates a flow exporter and enters flow exporter configuration mode.
Step 3	description string Example: 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] Example: 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 Example: 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 } Example: Switch(config-flow-exporter)# source gigabitEthernet1/0/1	
Step 7	transport udp number Example: 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

	Command or Action	Purpose
Step 8	ttl <i>seconds</i> Example: Switch(config-flow-exporter)# t11 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: Switch(config-flow-exporter)# export-protocol netflow-v9	Specifies the version of the NetFlow export protocol used by the exporter.
Step 10	end Example: Switch(config-flow-record)# end	Returns to privileged EXEC mode.
Step 11	show flow exporter [<i>name record-name</i>] Example: Switch# show flow exporter ExportTest	(Optional) Displays information about NetFlow flow exporters.
Step 12	copy running-config startup-config Example: 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.

Related Topics

[Exporters](#)

[Example: Configuring a Flow](#), on page 23

Creating a Customized 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 one of the predefined formats or 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 instead of using one of the Flexible NetFlow predefined records, 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 Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	flow monitor <i>monitor-name</i> Example: <pre>Device(config)# flow monitor FLOW-MONITOR-1</pre>	Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow monitor.
Step 4	description <i>description</i> Example: <pre>Device(config-flow-monitor)# description Used for basic ipv4 traffic analysis</pre>	(Optional) Creates a description for the flow monitor.
Step 5	record { <i>record-name</i> } Example: <pre>Device(config-flow-monitor)# record FLOW-RECORD-1</pre>	Specifies the record for the flow monitor.
Step 6	cache { <i>entries number</i> timeout { active inactive update } <i>seconds</i> { normal } Example:	(Optional) Modifies the flow monitor cache parameters such as timeout values, number of cache entries, and the cache type. <ul style="list-style-type: none"> • timeout active <i>seconds</i>—Configure the active flow timeout. This defines the

	Command or Action	Purpose
		<p>granularity of the traffic analysis. The range is from 1 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.</p> <p>Note Although visible in the command line help, the entries keyword and inactive and update timeouts are not supported.</p>
Step 7	Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor.	—
Step 8	<p>exporter <i>exporter-name</i></p> <p>Example:</p> <pre>Device(config-flow-monitor)# exporter EXPORTER-1</pre>	(Optional) Specifies the name of an exporter that was created previously.
Step 9	<p>end</p> <p>Example:</p> <pre>Device(config-flow-monitor)# end</pre>	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.
Step 10	<p>show flow monitor [[name] <i>monitor-name</i> [cache [format {csv record table}]]]</p> <p>Example:</p> <pre>Device# show flow monitor FLOW-MONITOR-2 cache</pre>	<p>(Optional) Displays the status for a Flexible NetFlow flow monitor.</p> <p>Note To sort by CTS flow source or destination tags, enter the show flow monitor <i>monitor-name</i> cache sort flow cts {source destination} group-tag format {csv record table} command.</p>
Step 11	<p>show running-config flow monitor <i>monitor-name</i></p> <p>Example:</p> <pre>Device# show running-config flow monitor FLOW_MONITOR-1</pre>	(Optional) Displays the configuration of the specified flow monitor.
Step 12	<p>copy running-config startup-config</p> <p>Example:</p>	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	Device# copy running-config startup-config	

Creating a Flow Sampler

Perform this required task to configure and enable a flow sampler.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	sampler <i>sampler-name</i> Example: Device(config)# sampler SAMPLER-1	Creates a sampler and enters sampler configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing sampler.
Step 4	description <i>description</i> Example: Device(config-sampler)# description Sample at 50%	(Optional) Creates a description for the flow sampler.
Step 5	mode {random} 1 out-of <i>window-size</i> Example: Device(config-sampler)# mode random 1 out-of 2	Specifies the sampler mode and the flow sampler window size. <ul style="list-style-type: none"> • The range for the <i>window-size</i> argument is from 32 to 1022.
Step 6	exit Example: Device(config-sampler)# exit	Exits sampler configuration mode and returns to global configuration mode.
Step 7	interface <i>type number</i> Example:	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
	Device(config)# interface GigabitEthernet 0/0/0	
Step 8	{ip ipv6} flow monitor <i>monitor-name</i> [[sampler] <i>sampler-name</i>] {input output} Example: Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input	Assigns the flow monitor and the flow sampler that you created to the interface to enable sampling.
Step 9	end Example: Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.
Step 10	show sampler <i>sampler-name</i> Example: Device# show sampler SAMPLER-1	Displays the status and statistics of the flow sampler that you configured and enabled.

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 Example: Switch# configure terminal	Enters global configuration mode.
Step 2	interface <i>type</i> Example: Switch(config)# interface GigabitEthernet1/0/1	Enters interface configuration mode and configures an interface. 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} <i>name</i> [[sampler <i>name</i>] {input output}] Example: Switch(config-if)# ip flow monitor	Associate an IPv4 or an IPv6 flow monitor, and an optional sampler to the interface for input or output packets. You can associate multiple monitors to an interface in both input and output directions.

	Command or Action	Purpose
	<code>MonitorTest input</code>	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. 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: <code>Switch(config-flow-monitor)# end</code>	Returns to privileged EXEC mode.
Step 5	show flow interface [interface-type number] Example: <code>Switch# show flow interface</code>	(Optional) Displays information about NetFlow on an interface.
Step 6	copy running-config startup-config Example: <code>Switch# copy running-config startup-config</code>	(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 2: Flexible NetFlow Monitoring Commands

Command	Purpose
<code>show flow exporter [broker export-ids name name statistics templates]</code>	Displays information about NetFlow flow exporters and statistics.
<code>show flow exporter [name exporter-name]</code>	Displays information about NetFlow flow exporters and statistics.

Command	Purpose
show flow interface	Displays information about NetFlow interfaces.
show flow monitor [name <i>monitor-name</i>]	Displays information about NetFlow flow monitors and statistics.
show flow monitor statistics	Displays the statistics for the flow monitor
show flow monitor <i>monitor-name</i> cache format { table record csv }	Displays the contents of the cache for the flow monitor, in the format specified.
show flow record [name <i>record-name</i>]	Displays information about NetFlow flow records.
show sampler [broker name <i>name</i>]	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
```

Related Topics

[Creating a Flow Record](#), on page 13

[User-Defined Records](#), on page 5

[Creating a Flow Exporter](#), on page 15
[Exporters](#)
[Creating a Flow Monitor](#)
[Monitors](#)

Additional References for NetFlow

Related Documents

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

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

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support