Configuring NetFlow

NetFlow identifies packet flows for ingress IP packets and provides statistics based on these packet flows. NetFlow does not require any change to either the packets themselves or to any networking device.

NetFlow Overview

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 (or VLAN) 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.

Cisco NX-OS supports both Traditional Netflow and Flexible NetFlow.

With Traditional NetFlow all of the keys and fields that are exported must be fixed. Traditional Netflow supports IPv4 flows only. You can choose which keys you want to use to define the flow. Each unique flow is cached and some statistics are collected for the flow.

Flexible NetFlow 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 NetFlow cache.

The flow record determines the type of data to be collected for a flow. The flow monitor combines the flow record and flow exporter with the NetFlow cache information.

Cisco NX-OS gathers NetFlow statistics in sampled mode. This means that packets on the interface or subinterface are analyzed at the configured rate.

Flow Record

A flow record defines the keys that NetFlow uses to identify packets in the flow as well as other fields of interest that NetFlow gathers for the flow. You can define a flow record with any combination of keys and fields of interest. Cisco NX-OS supports a rich set of keys. A flow record also defines the types of counters gathered per flow. You can configure 32-bit or 64-bit packet or byte counters. The key fields are specified with the match keyword. The fields of interest and counters are specified under the match keyword.

Cisco NX-OS enables the following match fields as the defaults when you create a flow record:

- match interface input
- match interface output
- match flow direction

Flow Exporter

A flow exporter contains network layer and transport layer details for the NetFlow export packet. You can configure the following information in a flow exporter:

- Export destination IPv4 or IPv6 address
- Source interface
- UDP port number (where the collector is listening for NetFlow packets)
- Export format

Note NetFlow export packets use the IP address that is assigned to the source interface. If the source interface does not have an IP address assigned to it, the flow exporter will be inactive.

Cisco NX-OS exports data to the remote collector, using UDP frames, whenever a timeout occurs. By default, the flow timeout value is set to 15 seconds.

NetFlow Match Keys

To identify a flow you can choose one or more match keys as part of the flow record.

NetFlow supports the following match keys to identify flows:

- IPv4 source and IPv4 destination addresses

- IPv6 source and IPv6 destination addresses
- IPv6 flow label
- IPv6 options
- TOS field
- Layer 4 protocol
- Layer 4 source and destination ports

The following match keys are provided for Layer 2 NetFlow:

- MAC source and destination addresses
- Ethertype
- VLAN

Specifying the Match Parameters

You must configure at least one of the following match parameters for flow records:

Command	Purpose
match ip {**protocol** | **tos**} **Example:** `switch(config-flow-record)# match ip protocol`	Specifies the IP protocol or ToS fields as keys **Note** The **match transport destination-port** and the **match ip protocol** commands are required to export Layer 4 port data. The data is collected and displayed in the output of the **show hardware flow ip** command but is not collected and exported until you configure both commands.
match ipv4 {**destination address** | **source address**} **Example:** `switch(config-flow-record)# match ipv4 destination address`	Specifies the IPv4 source or destination address as a key.
match ipv6 {**destination address** | **source address** | **flow-label** | **opitons** } **Example:** `switch(config-flow-record)# match ipv6 flow label`	Specifies the IPv6 key.

Command	Purpose
match transport {**destination-port** | **source-port**} **Example:** `switch(config-flow-record)# match transport destination-port`	Specifies the transport source or destination port as a key. **Note** The **match transport destination-port** and the **match ip protocol** commands are required to export Layer 4 port data. The data is collected and displayed in the output of the **show hardware flow ip** command but is not collected and exported until you configure both commands.
match datalink {**mac source-address** | **mac destination-address** | **ethertype** | **vlan**} **Example:** `switch(config-flow-record)# match datalink ethertype`	Specifies the Layer 2 attribute as a key.

NetFlow Collect Parameters

NetFlow can collect the following parameters, and export the values in either version 5 (traditional NetFlow) or version 9 (flexible NetFlow) format.

Note Some of these fields might not be available in traditional NetFlow format.

- Number of Layer 3 bytes (in 64 bit values optionally)
- Number of packets (in 64 bit values optionally)
- Flow direction
- Flow sampler ID
- Interface type (input, output or both)
- System up time for the first or the last packet
- TCP flags

Specifying the Collect Parameters

You must configure at least one of the following collect parameters for flow records:

Command	Purpose

collect counter {**bytes** | **packets**} [**long**]
Example:
`switch(config-flow-record)#`
`switch(config-flow-record)# collect counter packets`
	Collects either packet-based or byte counters from the flow. You can optionally specify that 64-bit counters are used.

collect flow sampler id **Example:** `switch(config-flow-record)# collect flow sampler`	Collects the sampler identifier used for the flow.
collect timestamp sys-uptime {**first** | **last**} **Example:** `switch(config-flow-record)# collect timestamp sys-uptime last`	Collects the system up time for the first or last packet in the flow.
collect transport tcp flags **Example:** `switch(config-flow-record)# collect transport tcp flags`	Collects the TCP transport layer flags for the packets in the flow.
collect ip version **Example:** `switch(config-flow-record)# collect ip version`	Collects the IP version for the flow.

Sampled NetFlow

Cisco NX-OS supports sampled NetFlow. This feature samples incoming packets on an interface. The packets sampled then qualify to create flows. Sampled NetFlow reduces the amount of export data sent to the collector by limiting the number of packets that create flows and the number of flows. It is essential when flows are created on a line card or external device, instead of on the forwarding engine.

The sampling mode supported is M out of N (M:N), where M packets are selected randomly out of every N packets for sampling, and only those packets can create flows. The lowest possible sampling rate on the Cisco Nexus 6000 series is 1:64K packets. The following table shows the different packet rates for different port types when the sampling rate is set to 1:64K packets:

Port Speed	Number of packets using a 1:64K sampled packet rate
1 Gigabit	23
10 Gigabit	230
40 Gigabit	920

Note The values in the above table apply to 64 Byte sized packets. The values are different for different size of packets.

Guidelines and Limitations for NetFlow

NetFlow has the following configuration guidelines and limitations:

- In sampler mode using M:N, N must be a power of 2. For example 1024, 2048, or 4096.
- You must configure a source interface. If you do not configure a source interface, the flow exporter will remain in a disabled state.
- If you configure both NetFlow and SPAN on the same interface then only the SPAN configuration is applied and the NetFlow configuration is ignored.
- You must configure a valid record name for every flow monitor.
- The maximum number of supported NetFlow entries is 512,000.
- You cannot change the fields in a record that is applied on the monitor
- You cannot change the sampling mode value on a sampler that is applied on the monitor
- If NetFlow is configured on both SVI and a VLAN then only the routed packets are updated on the SVI NetFlow.
- NetFlow can cause high CPU loads, to prevent issues with the control plane the following limitations apply:
  - NetFlow can be configured in the Ingress direction only
  - NetFlow packets that reach the CPU are not policed by the ASIC
- Ingress layer 2 NetFlow is supported on the following types of interfaces:
  - Layer 2 switch interface/port channel
  - FEX interface
- Ingress layer 3 NetFlow is supported on the following types of interfaces:
  - Layer 3 interface/port channel
  - Layer 3 sub-interface/port channel sub-interface
  - SVI
- Ingress bridged NetFlow is supported on VLANs.

How to Configure NetFlow

To configure NetFlow on a switch you perform the following steps:

- Define a flow record by specifying key and non-key fields of interest.
- Define one or many flow exporters by specifying export format, protocol, destination and other parameters.
- Define a flow monitor based on the above flow record and flow exporter(s).
- Apply the flow monitor to an interface with a sampling method specified.

Enabling the NetFlow Feature

You must globally enable NetFlow before you can configure any flows.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**feature netflow** **Example:** `switch(config)# feature netflow`	Enables the NetFlow feature.

Creating a Flow Record

Before You Begin

Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**flow record***name* **Example:** `switch(config)# flow record IPv4Flow`	Creates a flow record and enters flow record configuration mode.

	Command or Action	Purpose
Step 3	**description***string* **Example:** `switch(config-flow-record)# description Ipv4flow`	Describes this flow record.
Step 4	**match***type* **Example:** `switch(config-flow-record)# match transport destination-port`	Specifies the match key.
Step 5	**collect***type* **Example:** `switch(config-flow-record)# collect counter packets`	Specifies the collection field.
Step 6	**exit** **Example:** `switch(config-flow-record)# exit`	Returns to global configuration mode.
Step 7	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Creating a Flow Exporter

The flow exporter configuration defines the export parameters for a flow and specifies reachability information for remote NetFlow collector.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**flow exporter***name* **Example:** `switch(config)# flow exporter flow-exporter-one`	Creates a flow exporter and enters flow exporter configuration mode. You can enter up to 63 alphanumeric characters for the flow exporter name.

	Command or Action	Purpose
Step 3	**destination** { **ipv4-address** | **ipv6-address**} [**use-vrf** *name*] **Example:** `switch(config-flow-exporter)# destination 192.0.2.1`	Sets the destination IPv4 or IPv6 address for this flow exporter. You can optionally configure the VRF to use to reach the NetFlow collector. You can enter up to 32 alphanumeric characters for the VRF name.
Step 4	**source interface-type** *name/port* **Example:** `switch(config-flow-exporter)# source ethernet 2/1`	Specifies the interface to use to reach the NetFlow collector at the configured destination.
Step 5	**description** *string* **Example:** `switch(config-flow-exporter)# description exportversion9`	(Optional) (Optional) Describes this flow exporter. You can enter up to 63 alphanumeric characters for the description.
Step 6	**dscp** *value* **Example:** `switch(config-flow-exporter)# dscp 0`	(Optional) (Optional) Specifies the differentiated services codepoint value. The range is from 0 to 63.
Step 7	**transport udp** *port* **Example:** `switch(config-flow-exporter)# transport udp 200`	(Optional) (Optional) Specifies the UDP port to use to reach the NetFlow collector. The range is from 0 to 65535. **Note** If you do not specify the UDP port, 9995 is selected as the default.
Step 8	**version** {**5** | **9**} **Example:** `switch(config-flow-exporter)# version 9`	Specifies the NetFlow export version. Choose version 9 to enter the flow exporter version 9 configuration submode.
Step 9	**option** {**exporter-stats** | **interface-table** | **sampler-table**} **timeout** *seconds* **Example:** `switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200`	(Optional) Sets the flow exporter statistics resend timer. The range is from 1 to 86400 seconds.
Step 10	**template data timeout** *seconds* **Example:** `switch(config-flow-exporter-version-9)# template data timeout 1200`	(Optional) Sets the template data resend timer. The range is from 1 to 86400 seconds.
Step 11	**exit** **Example:** `switch(config-flow-exporter-version-9)# exit`	Returns to flow exporter configuration mode.

	Command or Action	Purpose
Step 12	**exit** **Example:** `switch(config-flow-exporter)# exit`	Returns to global configuration mode.
Step 13	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Creating a Flow Monitor

You can create a flow monitor and associate it with a flow record and a flow exporter. All the flows that belong to a monitor use the associated flow record to match on the different fields and the data is exported to the specified flow exporter.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**flow monitor***name* **Example:** `switch(config)# flow monitor flow-monitor-one`	Creates a flow monitor and enters flow monitor configuration mode. You can enter up to 63 alphanumeric characters for the flow monitor name.
Step 3	**description** *string* **Example:** `switch(config-flow-monitor)# description IPv4Monitor`	(Optional) Describes this flow monitor. You can enter up to 63 alphanumeric characters for the description.
Step 4	**exporter** *name* **Example:** `switch(config-flow-monitor)# export v9`	(Optional) Associates a flow exporter with this flow monitor. You can enter up to 63 alphanumeric characters for the exporter name.

	Command or Action	Purpose
Step 5	**record** {*name* **netflow-original** | **netflow protocol-port** | **netflow** {**ipv4** | **ipv6**} {**original-input** | **original-output**}} **Example:** `switch(config-flow-monitor)# record IPv4Flow`	Associates a flow record with the specified flow monitor. You can enter up to 63 alphanumeric characters for the record name.
Step 6	**exit** **Example:** `switch(config-flow-monitor)# exit`	Returns to global configuration mode.
Step 7	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Creating a Sampler

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

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**sampler** *name* **Example:** `switch(config)# sampler testsampler`	Creates a sampler and enters flow sampler configuration mode. You can enter up to 63 alphanumeric characters for the flow sampler name.
Step 3	**description** *string* **Example:** `switch(config-flow-sampler)# description samples`	(Optional) (Optional) Describes this sampler. You can enter up to 63 alphanumeric characters for the description.
Step 4	**mode** *sample-number* **out-of** *packet-number* **Example:** `switch(config-flow-sampler)# mode 1 out-of 128`	Defines the number of samples to take per the number of packets received. The sample-number range is from 1 to 64, and the packet-number range is from 1 to 65536 packets.

	Command or Action	Purpose
Step 5	**exit** **Example:** `switch(config-flow-sampler)# exit`	Returns to global configuration mode.
Step 6	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Applying a Flow Monitor to an Interface

Note You can not apply a flow monitor to an egress interface, only ingress Netflow is supported.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *interface-type slot/port* **Example:** `switch(config)# interface ethernet 2/1`	Enters interface configuration mode. The interface type can be Ethernet (including subinterfaces), port channel, or VLAN interface.
Step 3	**ip flow monitor** *name* **input sampler** *name* **Example:** `switch(config-if)# ip flow monitor testmonitor input sampler testsampler`	Associates an IPv4 flow monitor and a sampler to the interface for input packets. You can enter up to 63 alphanumeric characters for the flow monitor name and the sampler name.
Step 4	**ipv6 flow monitor** *name* **input sampler** *name* **Example:** `switch(config-if)# ipv6 flow monitor testmonitorv6 input sampler testsamplerv6`	Associates an IPv6 flow monitor and a sampler to the interface for input packets. You can enter up to 63 alphanumeric characters for the flow monitor name and the sampler name.
Step 5	**layer2-switched flow monitor** *name* **input sampler** *name*	Associates a Layer 2-switched flow monitor and a sampler to the interface for input packets. You can

	Command or Action	Purpose
	Example: `switch(config-if)# layer2-switched flow monitor testmonitorl2 input sampler testsamplerl2`	enter up to 63 alphanumeric characters for the flow monitor name and the sampler name.
Step 6	**exit** **Example:** `switch(config-if)# exit`	Returns to global configuration mode.
Step 7	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Configuring Bridged NetFlow on a VLAN

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

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**vlan configuration** *vlan-id* **Example:** `switch(config)# vlan configuration 30`	Enters VLAN configuration mode. The vlan-id range is from 1 to 3967 or from 4048 to 4093. **Note** VLAN configuration mode enables you to configure VLANs independently of their creation, which is required for VTP client support.
Step 3	{**ip ipv6**} **flow monitor** *name* **input sampler** *name* **Example:** `switch(config-vlan-config)# ip flow monitor testmonitor input sampler testsampler`	Associates a flow monitor and a sampler to the VLAN for input packets. You can enter up to 63 alphanumeric characters for the flow monitor name and the sampler name.
Step 4	**exit** **Example:** `switch(config-vlan-config)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Configuring NetFlow Timeouts

You can optionally configure global NetFlow timeouts that apply to all flows in the system.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**flow timeout***seconds* **Example:** `switch(config)# flow timeout 30`	Sets the flush timeout value in seconds. The range is from 5 to 60 seconds.
Step 3	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Verifying the NetFlow Configuration

To display the NetFlow configuration, perform one of the following tasks:

Command	Purpose
show flow exporter [*name*]	Displays information about NetFlow flow exporters and statistics. You can enter up to 63 alphanumeric characters for the flow exporter name.
show flow interface [*interface-type slot/port*]	Displays information about NetFlow interfaces.

Command	Purpose
show flow record [*name*]	Displays information about NetFlow flow records. You can enter up to 63 alphanumeric characters for the flow record name.
show flow record netflow layer2-switched input	Displays information about the Layer 2 NetFlow configuration.
show flow timeout	Displays information about NetFlow timeouts.
show sampler [*name*]	Displays information about NetFlow samplers. You can enter up to 63 alphanumeric characters for the sampler name.

Monitoring NetFlow

Use the **show flow exporter** command to display NetFlow statistics. Use the **clear flow exporter** command to clear NetFlow flow exporter statistics.

Configuration Examples for NetFlow

Example: Creating and Applying a Flow

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

```
feature netflow
flow exporter ee
 version 9
flow record rr
 match ipv4 source address
 match ipv4 destination address
 collect counter bytes
 collect counter packets
flow monitor foo
 record rr
 exporter ee
sampler testsampler
 mode 1 out-of 65536
interface Ethernet2/45
 ip flow monitor foo input sampler testsampler
 ip address 10.20.1.1/24
 no switchport
```

Example: Configuring a NetFlow Exporter

This example shows how to configure a NetFlow exporter configuration for IPv4 :

```
flow exporter pw
  destination 172.20.101.87 use-vrf management
  transport udp 3000
```

```
  source mgmt0
  version 9
flow record pw
  match ipv4 source address
  match ipv4 destination address
  match ip protocol
  match ip tos
  match transport source-port
  match transport destination-port
  collect counter bytes long
  collect counter packets long
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
  collect ip version
sampler testsampler
 mode 1 out-of 65536
flow monitor pw
  record pw
  exporter pw
interface Ethernet2/9
  ip flow monitor pw input sampler testsampler
```