Configuring NetFlow

This chapter describes how to configure the NetFlow feature on Cisco NX-OS devices.

- Finding Feature Information, on page 1
- NetFlow, on page 1
- Licensing Requirements for NetFlow, on page 6
- Prerequisites for NetFlow, on page 6
- Guidelines and Limitations for NetFlow, on page 6
- Default Settings for NetFlow, on page 9
- Configuring NetFlow, on page 9
- Verifying the NetFlow Configuration, on page 21
- Monitoring NetFlow, on page 22
- Configuration Examples for NetFlow, on page 22
- Verification Examples for NetFlow CoPP Interface Support , on page 23
- Related Documents, on page 23
- Feature History for NetFlow, on page 24

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch and the release notes for your 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 “New and Changed Information” chapter or the Feature History table.

NetFlow

NetFlow identifies packet flows for both ingress and egress IP packets and provide 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 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 NetFlow cache.

You can export the data that NetFlow gathers for your flow by using a flow exporter and export this data to a remote NetFlow collector. Cisco NX-OS exports a flow as part of a NetFlow export User Datagram Protocol (UDP) datagram under the following circumstances:

- The flow has been inactive or active for too long.
- The flow cache is getting full.
- One of the counters (packets or bytes) has exceeded its maximum value.
- You have forced the flow to export.

The flow record determines the size of the 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 can gather NetFlow statistics in either full or sampled mode. Cisco NX-OS analyzes all packets on the interface or subinterface for full NetFlow mode. For sampled mode, you configure the rate at which Cisco NX-OS analyzes packets.

Flow Records

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 **collect** 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 Exporters

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 IP address
- Source interface
- UDP port number (where the collector is listening for NetFlow packets)

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 collector whenever a timeout occurs or when the flow is terminated (TCP FIN or RST received, for example). You can configure the following timers to force a flow export:

- Active timeout—Removes the cache entries from the cache. Prevents long-lasting flows from becoming invisible to the collector for a long period of time. The value of the active timeout should always be greater than that of the inactive timeout. Active timeout is supported on the M1, M2, F3 and M3 Series modules.
- Inactive timeout—Removes the cache entries from the cache. Inactive timeout is supported on the M1, M2, F3 and M3 Series modules.
- Fast timeout—Flushes low-hitting flows for the M1 and M2 Series modules.
- Aggressive timeout—Aggressively times out the flows when the cache starts getting full for the M1 and M2 Series modules.
- Session timeout—Ages the flows if the TCP close connection handshake is observed (FIN/FIN_ACK packets). Session timeout is supported on M1 and M2 Series modules.
- Flush cache timeout—Flushes the cache for F2, F2e, and F3 Series modules.

Note The first five timeouts are applicable only to the NetFlow cache on M Series modules. The flow timeout is supported only for F2, F2e, and F3 Series modules.

The active and inactive timeouts exist by default and cannot be unconfigured. Only their time values can be configured.

Export Formats

Cisco NX-OS supports the Version 5 and Version 9 export formats. We recommend that you use the Version 9 export format for the following reasons:

- More efficient network utilization
- Support for IPv6 and Layer 2 fields

If you configure the Version 5 export format, you have these limitations:

- Fixed field specifications
- No support for IPv6 and Layer 2 fields

- The Netflow.InputInterface and Netflow.OutputInterface represent a 16-bit I/O descriptor (IOD) of the interface.

Note The IOD information of the interface can be retrieved using the show system internal im info global command.

Note Cisco NX-OS supports UDP as the transport protocol for exports to up to two collectors.

Note M1 Series modules support the configuration change from the Version 5 to Version 9 export format, but F2, F2e, and F3 Series modules do not.

Flow Monitors

A flow monitor references the flow record and flow exporter. You apply a flow monitor to an interface.

Samplers

Cisco NX-OS supports sampled NetFlow. This feature samples incoming and outgoing 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. F2, F2e, F3, and M3 Series modules support only sampled NetFlow.

Implementing NetFlow on F2 and F2e Series modules creates flows in the software. Too many packets trying to create or update flows can increase the load on the CPU, thereby increasing the need for a protective rate limiter. The rate limiter limits the number of packets that reach the CPU to approximately 1000 packets per second. F3 and M3 Series modules use a special hardware called FSA, which is used as a NetFlow processor, to create flows.

The sampling mode supported on F2, F2e, F3, M3, M1, and M2 modules is M out of N, where M packets are selected randomly out of every N packets for sampling, and only those packets can create flows.

Note With the F2 and F2e Series modules, you will need to be aware of the scaling factor to be configured, which is the additional sampling of 1:100 multiplied by the configured sampling. If you overlook this factor, you will not see the actual in the reported rate.

Rate limiter limits the number of packets that reach the CPU to approximately 1000 packets per second on the F2 and F2e Series modules. On the F3 Series module, rate limiting of 500 PPS per ASIC (SoC) is implemented. Hence, for Cisco NX-OS 7000, if the F3 Series module has 6 SoCs, then it will rate limit 500*6=3000 PPS to the CPU, per F3 Series module; and for Cisco NX-OS 7700, if the F3 Series module has 12 SoCs, then it will rate limit 500*12=6000 PPS to the CPU, per F3 Series module.

The F3 and M3 Series module supports more sampling rate, 1:131071 compared to 1:8191 on other F2 and F2e series modules.

Note The F3 series module supports an increased sampling rate on version 9. Performance on the F3 series module for the 7.2(0)D1(1) release has improved by 20 to 50 times the packet processing capability when compared to a 6.2.x release. It is enhanced to 50000 pps. Due to the increased speed, you can use a lower sampling rate on the F3 series module for this release. For example, a sampling of 1:4000 can be replaced with a sampling of 1:80.

On M3 series modules, the default rate limit value is 8000 PPS per ASIC (SoC). In such a scenario, the Cisco Nexus 7700 M3-Series 48-Port 1/10G Ethernet Module (with 2 SoCs) will rate limit 8000*2=16000 PPS only to the CPU per M3 Series module. Use the **hardware rate-limiter layer-2 netflow** *rate* **module** *m3module* command on a specific M3 Series module to configure the rate limit value to 24000 PPS. This configuration will enable the M3 series module to rate limit 24000*2=48000 PPS to the CPU per M3 Series module.

Similarly, the Cisco Nexus 7700 M3-Series 24-Port 40G Ethernet Module (with 4 SoCs) will rate limit 8000*4=32000 PPS only to the CPU per M3 Series module. Use the **hardware rate-limiter layer-2 netflow** *rate* **module** *m3module* command on a specific M3 Series module to configure the rate limit value to 12000 PPS. This configuration will enable the M3 Series module to rate limit 12000*4=48000 PPS to the CPU per M3 Series module.

The following limitations apply to sampled NetFlow and F2 Series and F2e Series modules:

- An additional sampling of 1:100 is applied over the configured value for F2 Series and F2e Series modules. For example, if the configured sampling is 1 in 200, the actual applied sampling is 1 in 20000. When you configure the sampler value to 1:4956, the system does not start the rate-limiter. This value is calculated based on the maximum traffic that would cross a module.
- The accuracy of the sampled NetFlow compared with the traditional NetFlow is dependent on the sampling rate configured. If the sampling rate is 1:1, the sampled NetFlow is exactly accurate as the traditional NetFlow. And if the sampling rate is 1:100, the sampled NetFlow is less accurate than the traditional, but it still yields statistical patterns that allow you to monitor the device.

Netflow on CoPP Interface Support

Netflow on CoPP Interface Support features enables application of Netflow on packets that are destined to the supervisor module, which is the control plane.

Netflow on CoPP Interface Support feature enables the monitoring of packets that are egressing to the control plane. This monitoring feature was added in NX-OS release 7.3(0)D1(1).

For more information on Control Plane Policing, See the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide*.

Network Analysis Module

You can also use the Cisco Network Analysis Module (NAM) to monitor NetFlow data sources. NAM enables traffic analysis views and reports such as hosts, applications, conversations, VLAN, and QoS. See the NAM configuration example in the Configuration Examples for NetFlow.

To use NAM for monitoring the Cisco Nexus 7000 NetFlow data sources, see the *Cisco Nexus 7000 Series Network Analysis Module (NAM-NX1) Quick Start Guide*.

High Availability

Cisco NX-OS supports stateful restarts for NetFlow. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

Because the flow cache is not preserved across restarts of the process and packets that come to the software during restarts cannot be processed, all of the flows during switchovers are lost and cannot be recovered.

Virtualization Support

A virtual device context (VDC) is a logical representation of a set of system resources. Within each VDC, you can configure NetFlow. By default, Cisco NX-OS places you in the default VDC and any flows that you define in this mode are only available for interfaces in the default VDC.

For information about configuring VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Licensing Requirements for NetFlow

Table 1: NetFlow Licensing Requirements

Product	License Requirement
Cisco NX-OS	NetFlow requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.

Prerequisites for NetFlow

NetFlow has the following prerequisites:

- You must understand the resources required on your device because NetFlow consumes additional memory and CPU resources.
- If you configure VDCs, install the appropriate license and enter the desired VDC. See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide for configuration information and the Cisco NX-OS Licensing Guide* for licensing information.

Guidelines and Limitations for NetFlow

NetFlow has the following configuration guidelines and limitations:

- MPLS-aware Netflow is *not* supported.

- You must configure a source interface for the NDE export. If you do not configure a source interface, the flow exporter will remain in a disabled state.
- You must configure a valid record name for every flow monitor.
- All of the NetFlow timeouts, except the flow timeout, are applicable only to M1 and M2 Series modules. The flow timeout is supported only for F2, F2e, and F3 Series modules. Only active and inactive timeouts are applicable for M3 Series modules.
- A rollback will fail if you try to modify a record that is programmed in the hardware during a rollback.
- Only Layer 2 NetFlow is applied on Layer 2 interfaces, and only Layer 3 NetFlow is applied on Layer 3 interfaces.
- If you add a member to a port channel that is already configured for Layer 2 NetFlow, its NetFlow configuration is removed and the Layer 2 configuration of the port channel is added to it.
- If you change a Layer 2 interface to a Layer 3 interface, the software removes the Layer 2 NetFlow configuration from the interface.
- Use NetFlow v9 export to see the full 32-bit SNMP ifIndex values at the NetFlow connector.
- The maximum number of supported NetFlow entries is 512,000.
- On tunnel interface, NetFlow is not supported, even though its configurable.
- The Cisco Nexus 2000 Series Fabric Extender (FEX) supports a Layer 3 NetFlow configuration on FEX ports.
- The Cisco Nexus 2000 Series FEX supports bridged NetFlow (for flows within a VLAN).
- M1 Series modules support the configuration change from the Version 5 to Version 9 export format, but F2, F2e, and F3 Series modules do not.
- F2, F2e, F3, and M3 Series modules do not support the following changes:
  - Changing the fields in a record that is applied on the active monitor.
  - Changing the sampling mode value on a sampler that is applied on the active monitor.
- Beginning with Cisco NX-OS Release 5.2, NetFlow is supported on switch virtual interfaces (SVIs) for F1 Series ports, if at least one M1 Series module is present. SVI NetFlow is for traffic that is routed between VLANs.
- For M Series modules, if you apply a Layer 3 NetFlow input flow monitor to an SVI and apply a Layer 2 NetFlow input flow monitor to a Layer 2 interface such as a trunk that allows the same underlying VLAN, all input flows into both interfaces are reported by the Layer 2 NetFlow flow monitor only.
- F2, F2e, F3, and M3 Series modules support only sampled NetFlow.
- Beginning with Cisco NX-OS Release 6.1(2), sampled NetFlow is supported on F2 and F2e Series modules.
- Beginning with Cisco NX-OS Release 6.2(6), sampled NetFlow is supported on F3 Series modules.
- Egress NetFlow is not supported on F2, F2e modules, and on any mixed VDC the modules are present in.
- Beginning from Cisco NX-OS Release 7.2(0)D1(1), Egress NetFlow is supported on F3 modules.

- Beginning from Cisco NX-OS Release 7.2(1)D1(1), Sub-interfaces are supported on F2, F2e, and F3 series modules.
- Beginning from Cisco NX-OS Release 7.3(0)DX(1), ingress and egress NetFlow is supported on M3 Series modules.
- By default, you cannot use ingress NetFlow sampling and DHCP relay together on the same interface. However, beginning with Cisco NX-OS Release 6.2(2), you can override the default and configure these two features on the same interface using the **hardware access-list resource feature bank-mapping command**, after you have entered the necessary commands to enable each of these features individually. For more information on this command, see the **Configuring IP ACLs** chapter of the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide*.
- Beginning with Cisco NX-OS Release 6.2(2), full NetFlow is supported on the Cisco NetFlow Generation Appliance (NGA) through SPAN. Sampled NetFlow is supported on the NGA through sampled SPAN.

NetFlow has the following limitations for mixed VDCs with both M1, M2 Series and F2, F2e, F3, and M3 Series modules:

- A VDC is classified as a mixed VDC only when it contains at least one F2e Series port or at least one F3 Series port.
- Layer 2 NetFlow—Sampled and full NetFlow is supported on the M1 and M2 Series module ports, and only sampled NetFlow is supported on the F2e, F3 and M3 Series module ports.
- Layer 3 NetFlow—Sampled and full NetFlow is supported on the M1 and M2 Series module ports. The F2 and F2e Series module ports come up in proxy mode and, therefore, cannot be configured as Layer 3 ports. Thus, Layer 3 NetFlow and subinterface NetFlow do not work with these ports. Sampled NetFlow is supported on F3 and M3 Series module ports.
- VLANs, SVIs, and port channels—Only sampled NetFlow is supported on VLANs, SVIs, and port channels for both the M1 and M2 Series and F2e, F3, and M3 Series modules.
- Subinterfaces (physical/port channels)—NetFlow configuration is supported on the F2, F2e, F3, and M3 Series module interfaces.
- Dynamic configuration change is not available in the mixed VDC for the policies applied on the M1 and M2 Series and F2e, F3, and M3 Series modules.
- Flow timeout applies only to the F2e and F3 Series modules. Other NetFlow timers apply to the M1 and M2 Series modules. Only active and inactive timeouts are applicable for M3 Series modules.
- Egress NetFlow is completely blocked in VDCs that contain both M Series and F2e and F3 Series modules.

Guidelines and Limitations Specific to NetFlow on CoPP Interface Support feature:

- The feature can be configured only on the default VDC.
- Only unicast packets are supported.
- The feature supports capture of Layer 3 NetFlow fields only. Capture of Layer 2 fields are not supported.
- The feature requires mandatory configuration of a sampler.
- After the feature is enabled, it is applied on all the line cards in the system as follows:
  - M1/M2 line cards create sampled flows in the hardware table. The global routing table, with 512,000 entries, is shared with the regular NetFlow.

- F2/F2e line cards create sampled flows in the software table. The limits on the size of packets per second (PPS) per table is shared with the regular NetFlow. An additional 1:100 sampler is also applicable as usual.
- F3 line cards create flows in the software. The limits on the size of PPS per table is shared with the regular NetFlow.
- The feature can be applied only in the egress direction, because the packets egress to the supervisor module.

Default Settings for NetFlow

The following table lists the default settings for NetFlow parameters.

Table 2: Default NetFlow Parameters

Parameters	Default
Egress and ingress cache size	512,000
Flow active timeout	1800 seconds
Flow timeout (for F2, F2e, and F3 Series modules only)	15 seconds
Flow timeout aggressive threshold	Disabled
Flow timeout fast threshold	Disabled
Flow timeout inactive	15 seconds
Flow timeout session aging	Disabled

Configuring NetFlow

To configure NetFlow, follow these steps:

Procedure

Step 1 Enable the NetFlow feature.

Step 2 Define a flow record by specifying keys and fields to the flow.

Step 3 Define an optional flow exporter by specifying the export format, protocol, destination, and other parameters.

Step 4 Define a flow monitor based on the flow record and flow exporter.

Step 5 Apply the flow monitor to a source interface, subinterface, VLAN interface.

Enabling the NetFlow Feature

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

Use the following command in global configuration mode to enable NetFlow:

Command	Purpose
feature netflow Example: `switch(config)# feature netflow`	Enables the NetFlow feature.

Command	Purpose
no feature netflow Example: `switch(config)# no feature netflow`	Disables the NetFlow feature. The default is disabled.

Creating a Flow Record

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

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 t**
	Example:
	`switch# config t`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`switch(config)#`
		Enters global configuration mode.

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

Step 3	(Optional) **description***string* **Example:** `switch(config-flow-record)# description Ipv4Flow`	(Optional) Describes this flow record as a maximum 63-character string.
Step 4	(Optional) **match***type*	Specifies a match key.

	Command or Action	Purpose
	Example: `switch(config-flow-record)# match transport destination-port`	**Note** The **match transport destination-port** and the **match ip protocol** commands are required to export Layer 4 port data.
Step 5	**collect** *type* **Example:** `switch(config-flow-record)# collect counter packets`	(Optional) Specifies the collection field.
Step 6	**show flow record** [**name**] [*record-name*] |**netflow-original** | **netflow protocol-port** | **netflow {ipv4** | **ipv6**} {**original-input** | **original-output**}} **Example:** `switch(config-flow-exporter)# show flow record netflow protocol-port`	(Optional) Displays information about NetFlow flow records. You can enter up to 63 alphanumeric characters for the flow record name.
Step 7	**copy running-config startup-config** **Example:** `switch(config-flow-exporter)# copy running-config startup-config`	(Optional) Saves this configuration change.

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.

Command	Purpose
match ipv6 {**destination address** | **source address** | **flow-label** | **opitons** } **Example:** `switch(config-flow-record)# match ipv6 flow label`	Specifies the IPv6 key.
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.

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.

Command	Purpose
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.

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.
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	(Optional) **description** *string* **Example:** `switch(config-flow-exporter)# description exportversion9`	(Optional) Describes this flow exporter. You can enter up to 63 alphanumeric characters for the description.

	Command or Action	Purpose
Step 6	(Optional) **dscp** *value* **Example:** `switch(config-flow-exporter)# dscp 0`	(Optional) Specifies the differentiated services codepoint value. The range is from 0 to 63.
Step 7	(Optional) **transport udp** *port* **Example:** `switch(config-flow-exporter)# transport udp 200`	(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	(Optional) **option** {**exporter-stats** | **interface-table** | **sampler-table**} **timeout** *seconds* **Example:** `switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200`	Sets the flow exporter statistics resend timer. The range is from 1 to 86400 seconds.
Step 10	(Optional) **template data timeout** *seconds* **Example:** `switch(config-flow-exporter-version-9)# template data timeout 1200`	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.
Step 12	**exit** **Example:** `switch(config-flow-exporter)# exit`	Returns to global configuration mode.
Step 13	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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	(Optional) **description** *string* **Example:** `switch(config-flow-monitor)# description IPv4Monitor`	Describes this flow monitor. You can enter up to 63 alphanumeric characters for the description.
Step 4	(Optional) **exporter** *name* **Example:** `switch(config-flow-monitor)# export v9`	Associates a flow exporter with this flow monitor. You can enter up to 63 alphanumeric characters for the exporter name.
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	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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	(Optional) **description** *string* **Example:** `switch(config-flow-sampler)# description samples`	(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.
Step 5	**exit** **Example:** `switch(config-flow-sampler)# exit`	Returns to global configuration mode.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
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* **Example:** `switch(config-if)# layer2-switched flow monitor testmonitorl2 input sampler testsamplerl2`	Associates a Layer 2-switched 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 6	**exit** **Example:** `switch(config-if)# exit`	Returns to global configuration mode.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Configuring Netflow on CoPP Interface Support

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

Before you begin

Perform the following configuration on the default VDC.

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Enter control-plane configuration mode. Enable users to associate attributes that are associated with the control plane of the device:

switch(config)# **control-plane**

Step 3 Associate an IPv4 flow monitor and a sampler to the control-plane for output packets. You can enter up to 63 alphanumeric characters for the flow monitor name and the sampler name:

switch(config-cp)# **ip flow monitor** *name* **output sampler** *name*

What to do next

You must perform the following tasks to complete configuring Netflow on COPP Interface Support feature:

Creating a Flow Record, on page 10

Creating a Flow Monitor

Creating a Sampler, on page 15

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:**	Returns to global configuration mode.

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

Configuring Layer 2 NetFlow

You can define Layer 2 keys in flexible NetFlow records that you can use to capture flows in Layer 2 interfaces. The Layer 2 keys are as follows:

- Source and destination MAC addresses
- Source VLAN ID
- EtherType from the Ethernet frame

You can apply Layer 2 NetFlow to the following interfaces for the ingress direction:

- Switch ports in access mode
- Switch ports in trunk mode
- Layer 2 port channels

Note You cannot apply Layer 2 NetFlow to VLANs, egress interfaces, or Layer 3 interfaces such as VLAN interfaces.

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 t**
	Example:
	`switch# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
		Enters global configuration mode.

Step 2	Required: **flow record** *name* **Example:** `switch(config)# flow record L2_record`	Enters flow record configuration mode. For more information about configuring flow records, see the "Creating a Flow Record" section.

	Command or Action	Purpose
Step 3	Required: **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.
Step 4	Required: **interface** {**ethernet** *slotport*} | {**port-channel** *number*} **Example:** `switch(config-flow-record)# interface Ethernet 6/3`	Enters interface configuration mode. The interface type can be a physical Ethernet port or a port channel.
Step 5	Required: **switchport** **Example:** `switch(config-if)# switchport`	Changes the interface to a Layer 2 physical interface. For information about configuring switch ports, see the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*.
Step 6	Required: **mac packet-classify** **Example:** `switch(config-if)# mac packet-classify`	Forces MAC classification of packets. For more information about using the mac packet-classify command, see the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide.* **Note** You must use this command to capture flows.
Step 7	Required: **layer2-switched flow monitor** *flow-name* **input** [**sampler** *sampler-name*] **Example:** `switch(config-vlan)# layer2-switched flow monitor L2_monitor input sampler L2_sampler`	Associates a flow monitor and an optional sampler to the switch port input packets. • You can enter up to 63 alphanumeric characters for the flow monitor name and the sampler name.
Step 8	Required: **show flow record netflow layer2-switched input** **Example:** `switch(config-if# show flow record netflow layer2-switched input`	(Optional) Displays information about the Layer 2 NetFlow default record.
Step 9	Required: **copy running-config startup-config** **Example:** `switch(config-vlan)# copy running-config startup-config`	(Optional) Saves this configuration change.

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	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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.
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.
show hardware ip flow	Displays information about NetFlow hardware IP flows.

Command	Purpose
show running-config netflow	Displays the NetFlow configuration that is currently on your device.

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

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

```
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
interface Ethernet2/45
 ip flow monitor foo input
 ip address 10.20.1.1/24
 no shutdown
```

This example shows a NetFlow exporter configuration for IPv4 from the Cisco Nexus 7000 Series switch to NAM:

```
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

flow monitor pw
  record pw
  exporter pw
```

```
interface Ethernet2/9
  ip flow monitor pw input
  ip flow monitor pw output
```

Verification Examples for NetFlow CoPP Interface Support

Sample Output for the show hardware flow ip Command

```
 switch(config-if)# show hardware flow ip

D - Direction; L4 Info - Protocol:Source Port:Destination Port
IF - Interface: (Eth)ernet, (S)vi, (V)lan, (P)ortchannel, (T)unnel
TCP Flags: Ack, Flush, Push, Reset, Syn, Urgent

D  IF          SrcAddr         DstAddr         L4 Info         PktCnt     TCP Fl
--+-----------+---------------+---------------+---------------+----------+------
CP sup-eth1    010.014.014.002 010.014.014.001 001:00000:00000 0000000021 ......
```

Sample Output for the show running-configuration netflow Command

```
 switch# show running-configuration netflow

version 7.3(0)D1(1)

feature netflow

flow timeout active 60
flow exporter exp1
  destination 10.76.80.132 use-vrf management
  transport udp 9995
  source mgmt0
  version 9
    template data timeout 5
    option sampler-table timeout 8
sampler s3
  mode 2 out-of 3
flow monitor M2
  record netflow ipv4 original-input
  exporter exp1
control-plane
  ip flow monitor M2 output sampler s3
```

Related Documents

Related Topic	Related Topic
NetFlow CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs and VRFs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*
Cisco Network Analysis Module (NAM)	*Cisco Network Analysis Module (NAM) for Nexus 7000 Quick Start Guide*

Cisco NetFlow Generation Appliance (NGA)	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*

Feature History for NetFlow

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 3: Feature History for NetFlow

Feature Name	Releases	Feature Information
NetFlow	7.3(2)D1(2)	The first switched and the last switched sizes are changed to 8 bytes (from 4 bytes).
NetFlow	7.3(0)DX(1)	Added support for NetFlow on M3 Series modules.
NetFlow	7.3(0)D1(1)	Added Netflow on CoPP Interface support.
NetFlow	7.2(0)D1(1)	Enhanced the F3 Series module packet processing rate to 50000 pps.
NetFlow	6.2(6)	Added support for F3 Series modules.
NetFlow	6.2(2)	Added support for ingress NetFlow sampling and DHCPrelay to be configured on the same interface.
NetFlow	6.2(2)	Added NAM support for NetFlow data sources.
NetFlow	6.2(2)	Added support for full NetFlow and sampled NetFlow on the Cisco NetFlow Generation Appliance (NGA).
NetFlow	6.1(2)	Added support for sampled NetFlow on F2 Series and F2eSeries modules.
NetFlow	6.1(2)	Added the flow timeout seconds command for F2 Series and F2e Series modules.
NetFlow	6.0(1)	NetFlow is not supported on F2 Series modules.

NetFlow	6.0(1)	Added support for the collect routing forwarding-status command to trigger the collection of flows denied by ACL entries.
NetFlow	5.2(1)	NetFlow is supported on switch virtual interfaces (SVIs) for F1 Series ports.
Bridged NetFlow	5.1(1)	VLAN configuration mode, which enables you to configure VLANs independently of their creation, is supported when configuring bridged NetFlow on a VLAN.
NetFlow verification	5.0(2)	You can specify the NetFlow instance for which you want to display NetFlow IPv4 flows and NetFlow table utilization.
Layer 2 NetFlow	4.2(1)	You can define Layer 2 keys in flexible NetFlow records that you can use to capture flows in Layer 2 interfaces.
Rollback during NetFlow	4.1(3)	Rollback fails for NetFlow if, during rollback, you try to modify a record that is programmed in the hardware.