Configuring NetFlow

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

About 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 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, such as Cisco Stealthwatch. Cisco NX-OS exports a flow as part of a NetFlow export User Datagram Protocol (UDP) datagram under the following circumstances:

- Flows are exported periodically as per the flow timeout value, which defaults to 10 seconds if not configured.
- 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 and analyze all packets on the interface or subinterface.

Dual-Layer NetFlow Implementation

Unlike other Cisco Nexus platforms, Cisco Nexus 9000 Series switches separate NetFlow processing into two layers:

- The first layer supports per-packet visibility for line-rate traffic. Packets do not need to be sampled and statistically analyzed. Instead, the packets can be processed and aggregated at line rate.
- The second layer enables the gathering of flows at scale. It can maintain hundreds of thousands of flows without losing any flows and periodically exports them to an external collector.

Flow Records

A flow record defines the keys that NetFlow uses to identify packets and 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- 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 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 NetFlow Collector is listening for NetFlow packets)—The default value is 9995.

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 drops flows that were meant to be exported.

Cisco NX-OS exports data to the NetFlow Collector whenever a timeout occurs. You can configure a flush cache timeout (using the **flow timeout** command) to flush the cache and force a flow export.

Export Format

Cisco NX-OS supports the Version 9 export format. This format supports a more efficient network utilization than the older Version 5 export format and supports IPv6 and Layer 2 fields. In addition, the Version 9 export format supports the full 32-bit SNMP ifIndex values at the NetFlow Collector.

Layer 2 NetFlow Keys

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.

Flow Monitors

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

High Availability

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

The flow cache is not preserved across restarts, and packets that come to the software during restarts cannot be processed.

Prerequisites for NetFlow

NetFlow has the following prerequisites:

- Make sure that you understand the resources required on your device because NetFlow consumes memory and CPU resources.

Guidelines and Limitations for NetFlow

Note For scale information, see the release-specific *Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*.

NetFlow has the following configuration guidelines and limitations:

- The following switches support NetFlow:
  - Cisco Nexus 9300-FX platform switches, beginning with Cisco NX-OS Release 7.0(3)I7(1).
  - Cisco Nexus 9300-EX platform switches, beginning with Cisco NX-OS Release 7.0(3)I7(2).
  - Cisco Nexus 9336C-FX2, and 93240YC-FX2 switches, beginning with Cisco NX-OS Release 7.0(3)I7(3).
- Cisco Nexus 3232C, 3264Q, and 9364C switches do not support NetFlow.
- The following guidelines and limitations are applicable to Netflow in a VXLAN environment:
  - NetFlow is supported on SVI and non-uplink L3 Interfaces of a VXLAN VTEP. This does not include the L3VNI SVI.
  - NetFlow is not supported on uplink interfaces on a VXLAN VTEP.
  - NetFlow on Multisite Border Gateways is not supported.
  - A NetFlow Collector that is reachable over the VXLAN fabric is supported.
- NetFlow is not supported on tunnel interfaces.
- NetFlow for FEX Layer 3 ports is not supported.
- NetFlow is not supported for CPU-transmitted packets.
- Only ingress NetFlow is supported. Egress NetFlow is not supported.
- Flow cache can be cleared per flow type, such as Layer 2, IPv4, and IPv6. It cannot be cleared per flow monitor.
- Flow collection is not performed for ARP traffic.
- Collection of the OUTPUT_SNMP field is not supported for any Cisco Nexus 9000 platform switch or Cisco Nexus line card in Cisco NX-OS Release 7.x.
- You must configure a source interface for the NetFlow Data Export (NDE). If you do not configure a source interface, the flow exporter drops flows that were meant to be exported.
- Layer 2 switched flow monitors are applied only to Layer 2 interfaces. IP and IPv6 flow monitors can be applied to VLANs, SVIs, Layer 3 routed interfaces, or subinterfaces.
- If you change a Layer 2 interface to a Layer 3 interface, or a Layer 3 interface to a Layer 2 interface, the software removes the Layer 2 NetFlow configuration from the interface.
- A rollback fails if you try to modify a record that is programmed in the hardware during a rollback.

- For Cisco Nexus 9300-FX platform switches only, 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.
- On Cisco Nexus 9300-EX/FX/FX2 platform switches, SPAN, and sFlow cannot both be enabled simultaneously. If one is active, the other cannot be enabled. However, on the Cisco Nexus 9300-EX/FX/FX2, both NetFlow and SPAN can both be enabled simultaneously, providing a viable alternative to using sFlow and SPAN.
- For Cisco Nexus 9300-EX platform switches, a flow monitor applied on a VLAN or SVI can collect flows for both switched and routed traffic. For Cisco Nexus 9300-FX platform switches, NetFlow VLANs are supported for switched traffic only, and NetFlow SVIs are supported for routed traffic only.
- For Cisco Nexus 9300-EX platform switches, the same flow monitor cannot be attached to a VLAN and an SVI at the same time.
- The Cisco Nexus 9300-EX platform switches have dedicated TCAM and do not require carving.
- TCAM carving configuration of the ing-netflow region can be performed on -FX line cards. -EX line cards have a default ing-netflow region TCAM carving of 1024 and cannot be configured otherwise. For ports on the -EX and -FX line cards, the suggested maximum for the ing-netflow region is 1024.
- The ToS field is not exported for Cisco Nexus 9300-EX platform switches.
- Record match, based on IP ToS, is not supported for IPv6 flow monitors. The ToS value is collected on the collector as 0x0 irrespective of the value the traffic holds.

  This limitation is applicable for the following platform switch families:

  - Cisco Nexus 9300-EX
  - Cisco Nexus 9300-FX
  - Cisco Nexus 9300-FX2

- Cisco Nexus 9300-EX platform switches support only IPv4 and IPv6 flow monitors. Cisco Nexus 9300-FX platform switches support Layer 2, IPv4, and IPv6 flow monitors.
- For Cisco Nexus 9300-EX platform switches, you cannot apply Layer 2 flow monitors to Layer 2 interfaces.

Note For verified NetFlow scalability numbers, see the Cisco Nexus 9000 Series NX-OS Verified Scalability Guide.

Configuring NetFlow

Follow these steps to configure NetFlow:

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, or VLAN interface.

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	[**no**] **feature netflow** **Example:** `switch(config)# feature netflow`	Enables or disables the NetFlow feature. The default is disabled.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Creating a Flow Record

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

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 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.

	Command or Action	Purpose
Step 3	(Optional) **description** *string* **Example:** `switch(config-flow-record)# description IPv4Flow`	Describes this flow record as a maximum 63-character string.
Step 4	(Optional) **match** *type* **Example:** `switch(config-flow-record)# match transport destination-port`	Specifies a match key. For more information, see Specifying the Match Parameters, on page 7. **Note** The **match transport destination-port** and **match ip protocol** commands are required to export Layer 4 port data.
Step 5	(Optional) **collect** *type* **Example:** `switch(config-flow-record)# collect counter packets`	Specifies the collection field. For more information, see Specifying the Collect Parameters, on page 8.
Step 6	(Optional) **show flow record** [*name*] [*record-name*] {**netflow-original** | **netflow protocol-port** | **netflow** {**ipv4** | **ipv6**} {**original-input** | **original-output**}} **Example:** `switch(config-flow-record)# show flow record netflow protocol-port`	Displays information about NetFlow flow records. You can enter up to 63 alphanumeric characters for the flow record name.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config-flow-record)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Specifying the Match Parameters

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

Command	Purpose
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.

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 **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** | **options**} **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 **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.

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)# collect counter packets`	Collects either packet-based or byte counters from the flow. You can optionally specify that 64-bit counters are used.

Command	Purpose
collect ip version **Example:** `switch(config-flow-record)# collect ip version`	Collects the IP version 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.

Creating a Flow Exporter

The flow exporter configuration defines the export parameters for a flow and specifies reachability information for the 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`
	`switch(config-flow-exporter)#`
		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.

	Command or Action	Purpose
Step 5	(Optional) **description** *string* **Example:** `switch(config-flow-exporter)# description exportversion9`	Describes this flow exporter. You can enter up to 63 alphanumeric characters for the description.
Step 6	(Optional) **dscp** *value* **Example:** `switch(config-flow-exporter)# dscp 0`	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`	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 9**
	Example:
	`switch(config-flow-exporter)# version 9`
	`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**} **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	(Optional) **copy running-config startup-config** **Example:** `switch(config-flow-exporter-version-9)# copy running-config startup-config`	Copies 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 of 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`
	`switch(config-flow-monitor)#`
		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	(Optional) **copy running-config startup-config** **Example:** `switch(config-flow-monitor)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Applying a Flow Monitor to an Interface

You can apply a flow monitor to an ingress interface. Egress Netflow is not supported.

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose

Step 2	**interface vlan** *vlan-id*
	Example:
	`switch(config)# interface vlan 10`
	`switch(config-if)#`
		Configures a VLAN interface and enters interface configuration mode.

Step 3	**ip flow monitor** {**ipv4** | **ipv6** | **layer-2-switched**} **input** **Example:** `switch(config-if)# ip flow monitor ipv4 input`	Associates an IPv4, IPv6, or Layer 2-switched flow monitor to the interface for input packets.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Bridged NetFlow on a VLAN

You can apply a flow monitor to a VLAN in order to gather Layer 3 data over Layer 2 switched packets in 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`
	`switch(config-vlan-config)#`
		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* **Example:** `switch(config-vlan-config)# ip flow monitor testmonitor`	Associates a flow monitor to the VLAN for input packets. You can enter up to 63 alphanumeric characters for the flow monitor name.
Step 4	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	`switch(config-vlan-config)# copy running-config startup-config`	

Configuring Layer 2 NetFlow Keys

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

Procedure

	Command or Action	Purpose

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

Step 2	**flow record** *name*
	Example:
	`switch(config)# flow record L2_record`
	`switch(config-flow-record)#`
		Enters flow record configuration mode. For more information about configuring flow records, see Creating a Flow Record, on page 6.

Step 3	**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	**exit**
	Example:
	`switch(config-flow-record)# exit`
	`switch(config)#`
		Exits flow record configuration mode.

Step 5	**interface** {**ethernet** *slot/port* | **port-channel** *number*}
	Example:
	`switch(config)# interface Ethernet 6/3`
	`switch(config-if#)`
		Enters interface configuration mode. The interface type can be a physical Ethernet port or a port channel.

Step 6	**switchport** **Example:** `switch(config-if)# switchport`	Changes the interface to a Layer 2 physical interface. For information on configuring switch ports, see the Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide.
Step 7	**mac packet-classify** **Example:** `switch(config-if)# mac packet-classify`	Forces MAC classification of packets. For more information on using this command, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

	Command or Action	Purpose
		Note You must use this command to capture flows.
Step 8	**layer2-switched flow monitor** *flow-name* **input** **Example:** `switch(config-if)# layer2-switched flow monitor L2_monitor input`	Associates a flow monitor to the switch port input packets. You can enter up to 63 alphanumeric characters for the flow monitor name.
Step 9	(Optional) **show flow record netflow layer2-switched input** **Example:** `switch(config-if)# show flow record netflow layer2-switched input`	Displays information about the Layer 2 NetFlow default record.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies 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. The default value is 10 seconds.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies 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 cache [**ipv4** | **ipv6** | **ce**]	Displays information about NetFlow IP flows.
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 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 Example for NetFlow

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

```
feature netflow
flow exporter ee
 destination 171.70.242.48 use-vrf management
 source mgmt0
 version 9
  template data timeout 20
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
```