



Configuring NetFlow

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

This chapter contains the following sections:

- [About NetFlow, on page 1](#)
- [Prerequisites for NetFlow, on page 4](#)
- [Guidelines and Limitations for NetFlow, on page 4](#)
- [Configuring NetFlow, on page 8](#)
- [Verifying the NetFlow Configuration, on page 18](#)
- [Monitoring NetFlow, on page 18](#)
- [Display Example for NetFlow, on page 18](#)
- [Configuration Example for NetFlow, on page 19](#)

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. The Netflow Exporter source interface and destination IP must use the same VRF.

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.

NetFlow Output Interface

The NetFlow output interface on Cisco Nexus 9300-FX/FX3 and Cisco Nexus 9500 platform switches with FM-E and FM-E2 modules have the following features:

- NetFlow in the **show flow cache** command displays `output_if_id` and exports output interface to the collector on Cisco Nexus 9300-FX and 9500 platform switches with 9700-EX line cards.
- The NetFlow output interface for Cisco Nexus 9300-FX/FX3 platform switches supports both IPv4 and IPv6 traffic flows. The NetFlow output interface for Cisco Nexus 9500 platform switches is supported only for IPv4 traffic flows and is not supported for IPv6 traffic flows.
- The **show flow cache** command displays `output_if_id` as `0x0`. Also note that this feature is supported for traffic other than traffic destined to the switch such as control plane traffic and ICMP request/reply messages.
- NetFlow supports exporting output interface to the collector for IPv4/IPv6 incoming traffic flows, which have Next-Hop as destination interface. The NetFlow export format for `InputInt` and `OutputInt` support the full 32-bit SNMP `ifIndex` values at the NetFlow Collector.

- The NetFlow output interface is not supported for tunnel traffic flows such as MPLS, VXLAN, and GRE.
- For more information on examples for NetFlow output interface, see the [Display Example for NetFlow, on page 18](#).

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:

- 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.
- NetFlow is not supported on tunnel interfaces.
- 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.
- 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.

- The same flow monitor cannot be shared with a VLAN and Layer 3 interfaces (for example, physical Layer 3 interface, SVI interface, or Layer 3 subinterface). You must distinguish a VLAN and Layer 3 interface since the ACL is different and cannot be shared. They must be treated as two different profiles.
- A rollback fails if you try to modify a record that is programmed in the hardware during a rollback.
- The limitations of the NetFlow feature are as follows:
 - NetFlow for MPLS/VXLAN datapath is not supported
 - NetFlow is not supported on loopback and switch management interfaces.
- 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.
- Beginning with Cisco NX-OS Release 9.2(1):
 - NetFlow for FEX Layer 3 ports is supported on Cisco Nexus 9300-EX and 9300-FX platform switches.
 - NetFlow CE is supported on the Cisco Nexus 9300-EX platform switches.



Note All EX type platform switches, including the Cisco Nexus 9700-EX line cards, CE NetFlow only captures CE flow records for non-IPv4 and IPv6 traffic flows. Whereas for FX and FX2 type platform switches and line cards, we can capture CE flow data for IP flows as long as **mac packet-classify** is applied on the interface.

- Beginning with Cisco NX-OS Release 9.2(2), the Cisco Nexus 9300-FX switch supports collecting the OUTPUT_SNMP field for NetFlow Data Export (NDE). No other Cisco Nexus 9000 platform switch or Cisco Nexus line card supports collecting the OUTPUT_SNMP field.
- Beginning with Cisco NX-OS Release 9.2(2), NetFlow is supported on Cisco Nexus 9500 platform switches with Cisco Nexus 9700-EX line cards and FM-E modules.
- NetFlow is not supported on Cisco Nexus 92348GC-X platform switch.
- 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.
- The Cisco Nexus 9300-EX platform switch supports NetFlow and SPAN on the same interface at the same time. This functionality is a viable alternative to using SPAN and sFlow.
- On Cisco Nexus 9300-EX/FX platform switches, and Cisco Nexus 9500 platform switches with EX/FX modules, 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 and the Cisco Nexus 9500 platform switches

with EX modules, both NetFlow and SPAN can be enabled simultaneously, providing a viable alternative to using sFlow and SPAN.



Note Cisco Nexus 9300-FX2 platform switches support sFlow and SPAN coexistence.

- 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 that is 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-FX3
 - Cisco Nexus 9300-GX
 - Cisco Nexus 9500 with EX and FX line cards
- The following guideline applies to all Cisco Nexus 9500 platform switches with EX and FX line cards:
Configuring an EX port as a trunk when FX ports are trunks with NetFlow configurations already applied, does not remove the unsupported EX NetFlow configuration from the FX port trunks. For example, if you apply more than two different IPv4 flow monitors to FX port trunks and if EX ports are added to the same trunks, the configuration on the trunks beyond the two monitors is not automatically removed, since it's only an EX port limitation. Since this configuration will not report flows beyond two monitors for EX trunk ports, we recommend that you use only two monitors per protocol (v4/v6/CE) on modular switches that could potentially have both EX and FX ports in the same trunk.
 -
 - Commands **record netflow ipv4 original-input**, **record netflow ipv4 original-output**, and **record netflow layer2-switched input** are not supported in Cisco NX-OS Release 9.3(1).
 - Beginning with Cisco NX-OS Release 9.3(3), the following Non-Disruptive In-Service Software Upgrade (ND ISSU) limitations about NetFlow apply for all Cisco Nexus 9000 Series switches:
 - While performing an ND ISSU, a two-minute export loss is expected.
 - During an ND ISSU, an exporter with a management interface source port is not supported. Export loss is expected until the management interface comes up.

- Beginning with Cisco NX-OS Release 9.3(3), ingress NetFlow is supported on Cisco Nexus 9300-GX platform switch.
- Beginning with Cisco NX-OS Release 9.3(4), the following RTP/NetFlow monitoring limitation exists:

The RTP monitoring feature enables a monitor of RTP flows on all interfaces of a switch and reports them in the **show flow rtp detail** command output. An RTP flow is any UDP flow with a source port within the range of 16384-32767. If a NetFlow monitor is attached to a switch interface with RTP monitoring enabled, then all the traffic/flows (including the RTP flows) on that interface are reported in the output of the **show flow cache** command. The RTP flows will no longer be shown in the output of the **show flow rtp detail** command. When the attached monitor is removed, the RTP flows are reported again in the **show flow rtp detail** command output.

This limitation impacts the following switches:

- Cisco Nexus 9336C-FX2
 - Cisco Nexus 93240YC-FX2
 - Cisco Nexus 9348GC-FXP
 - Cisco Nexus 93180YC-FX
 - Cisco Nexus 93108TC-FX
 - Cisco Nexus 9316D-GX
 - Cisco Nexus 93600CD-GX
 - Cisco Nexus 9364C-GX
 - Cisco Nexus 9504, 9508, and 9516 with the 9736C-FX line card
- Cisco Nexus 9500 platform switches with FM-E, FM-E2, and FM-E3 modules and Cisco Nexus 9300-FX/FX3 switches support the NetFlow output interface feature. However, output interface is not supported on 9300-EX and 9500-EX platform switches.
 - NetFlow is supported on Cisco Nexus 9500 platform switches with EX, FX, and GX mixed chassis. You can use SPAN simultaneously with NetFlow on the Cisco Nexus 9500 platform switches with EX, FX, and GX mixed chassis. Cisco Nexus 9500-GX platform switches does not support SPAN with sFlow feature mix.
 - The Cisco Nexus 3232C and 3264Q switches do not support NetFlow.
 - Beginning with Cisco NX-OS Release 10.1(2), Netflow is supported on N9K-X9716D-GX line card.
 - Enable NetFlow only on platforms that support this feature.
 - The **match ip tos** command is present in flow record configuration options, but the functionality is not supported.
 - Beginning with Cisco NX-OS Release 10.2(1)F, Layer 3 NetFlow on Layer 2 interfaces is supported on Cisco Nexus 9300-EX, 9300-FX, 9300-FX2, 9300-FX3, 9300-GX, and 9300-GX2 platform switches, and on 9500-EX LC and 9500-FX LC. Few guidelines and limitations are as follows:
 - You can attach either Layer 3 flow monitor or Layer 2 flow monitor to Layer 2 interface, not both.
 - If a flow monitor is already attached to Layer 3 interface, then the same flow monitor cannot be attached to Layer 2 interface.

- The **mac-packet-classify** command is not supported, when Layer 3 flow monitor is applied on Layer 2 interface.



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: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	[no] feature netflow Example: <pre>switch(config)# feature netflow</pre>	Enables or disables the NetFlow feature. The default is disabled. Note The Cisco Nexus 9500 platform switches with N9K-T2 EoR do not support NetFlow.
Step 3	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	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 <i>name</i> 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 <i>string</i> Example: switch(config-flow-record)# description IPv4Flow	Describes this flow record as a maximum 63-character string.
Step 4	(Optional) match <i>type</i> Example: switch(config-flow-record)# match transport destination-port	Specifies a match key. For more information, see Specifying the Match Parameters, on page 10 . Note The match transport destination-port and match ip protocol commands are required to export Layer 4 port data.
Step 5	(Optional) collect <i>type</i> Example: switch(config-flow-record)# collect counter packets	Specifies the collection field. For more information, see Specifying the Collect Parameters, on page 11 .
Step 6	(Optional) show flow record [<i>name</i>] [<i>record-name</i>] {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
<p>match datalink {mac source-address mac destination-address ethertype vlan}</p> <p>Example:</p> <pre>switch(config-flow-record)# match datalink ethertype</pre>	<p>Specifies the Layer 2 attribute as a key.</p>
<p>match ip {protocol tos}</p> <p>Example:</p> <pre>switch(config-flow-record)# match ip protocol</pre>	<p>Specifies the IP protocol or ToS fields as keys.</p> <p>Note The match transport destination-port and match ip protocol commands are required to export Layer 4 port data.</p> <p>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.</p>
<p>match ipv4 {destination address source address}</p> <p>Example:</p> <pre>switch(config-flow-record)# match ipv4 destination address</pre>	<p>Specifies the IPv4 source or destination address as a key.</p>
<p>match ipv6 {destination address source address flow-label options}</p> <p>Example:</p> <pre>switch(config-flow-record)# match ipv6 flow-label</pre>	<p>Specifies the IPv6 key.</p>
<p>match transport {destination-port source-port}</p> <p>Example:</p> <pre>switch(config-flow-record)# match transport destination-port</pre>	<p>Specifies the transport source or destination port as a key.</p> <p>Note The match transport destination-port and match ip protocol commands are required to export Layer 4 port data.</p> <p>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.</p>

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: <pre>switch(config-flow-record)# collect counter packets</pre>	Collects either packet-based or byte counters from the flow. You can optionally specify that 64-bit counters are used.
collect ip version Example: <pre>switch(config-flow-record)# collect ip version</pre>	Collects the IP version for the flow.
collect timestamp sys-uptime {first last} Example: <pre>switch(config-flow-record)# collect timestamp sys-uptime last</pre>	Collects the system up time for the first or last packet in the flow.
collect transport tcp flags Example: <pre>switch(config-flow-record)# collect transport tcp flags</pre>	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: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	flow exporter <i>name</i> Example: <pre>switch(config)# flow exporter flow-exporter-one switch(config-flow-exporter)#</pre>	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 { <i>ipv4-address</i> <i>ipv6-address</i> } [use-vrf <i>name</i>] Example:	Sets the destination IPv4 or IPv6 address for this flow exporter. You can optionally configure the VRF to use to reach the NetFlow

	Command or Action	Purpose
	<code>switch(config-flow-exporter)# destination 192.0.2.1</code>	Collector. You can enter up to 32 alphanumeric characters for the VRF name.
Step 4	source <i>interface-type name/port</i> Example: <code>switch(config-flow-exporter)# source ethernet 2/1</code>	Specifies the interface to use to reach the NetFlow Collector at the configured destination.
Step 5	(Optional) description <i>string</i> Example: <code>switch(config-flow-exporter)# description exportversion9</code>	Describes this flow exporter. You can enter up to 63 alphanumeric characters for the description.
Step 6	(Optional) dscp <i>value</i> Example: <code>switch(config-flow-exporter)# dscp 0</code>	Specifies the differentiated services codepoint value. The range is from 0 to 63.
Step 7	(Optional) transport udp <i>port</i> Example: <code>switch(config-flow-exporter)# transport udp 200</code>	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: <code>switch(config-flow-exporter)# version 9</code> <code>switch(config-flow-exporter-version-9)#</code>	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 <i>seconds</i> Example: <code>switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200</code>	Sets the flow exporter statistics resend timer. The range is from 1 to 86400 seconds.
Step 10	(Optional) template data timeout <i>seconds</i> Example: <code>switch(config-flow-exporter-version-9)# template data timeout 1200</code>	Sets the template data resend timer. The range is from 1 to 86400 seconds.
Step 11	(Optional) copy running-config startup-config Example: <code>switch(config-flow-exporter-version-9)# copy running-config startup-config</code>	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. Note record netflow ipv4 original-input, record netflow ipv4 original-output, and record netflow layer2-switched input are not supported in Cisco NX-OS Release 9.3(1).
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: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	interface vlan <i>vlan-id</i> Example: <pre>switch(config)# interface vlan 10 switch(config-if)#</pre>	Configures a VLAN interface and enters interface configuration mode.
Step 3	ip flow monitor {ipv4 ipv6 layer-2-switched} input Example: <pre>switch(config-if)# ip flow monitor ipv4 input</pre>	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: <pre>switch(config-if)# copy running-config startup-config</pre>	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: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	vlan configuration <i>vlan-id</i> Example: <pre>switch(config)# vlan configuration 30 switch(config-vlan-config)#</pre>	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.

	Command or Action	Purpose
Step 3	{ip ipv6} flow monitor <i>name</i> 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: switch(config-vlan-config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

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 <i>name</i> 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 9 .
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 <i>slot/port</i> port-channel <i>number</i>} 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.

	Command or Action	Purpose
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 . Note You must use this command to capture flows.
Step 8	layer2-switched flow monitor <i>flow-name</i> 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 Layer 3 NetFlow on Layer 2 Interfaces

You can define Layer 3 flow monitors on Layer 2 interfaces to capture Layer 3 flow information on Layer 2 interfaces.

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	flow record <i>name</i> Example: switch(config)# flow record L3_record switch(config-flow-record)#	Enters flow record configuration mode. For more information about configuring flow records, see Creating a Flow Record, on page 9 .
Step 3	interface { <i>ethernet slot/port</i> 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 4	switchport Example: switch(config-if)# switchport	Changes the interface to a Layer 2 mode. For information on configuring switch ports, see the Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide .
Step 5	ip flow monitor <i>flow-name</i> input Example: switch(config-if)# ip flow monitor v41 input	Associates an IPv4 flow monitor to the switch port input packets. You can enter up to 63 alphanumeric characters for the flow monitor name.
Step 6	ipv6 flow monitor <i>flow-name</i> input Example: switch(config-if)# ipv6 flow monitor v61 input	Associates an IPv6 flow monitor to the switch port input packets. You can enter up to 63 alphanumeric characters for the flow monitor name.
Step 7	(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 <i>seconds</i> 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.

	Command or Action	Purpose
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.

Display Example for NetFlow

The output of the **show flow cache** command for IPv4 displays:

```
show flow cache
IPV4 Entries
SIP      DIP      BD ID  S-Port  D-Port  Protocol  Byte Count  Packet Count  TCP FLAGS
TOS  if_id  output_if_id  flowStart flowEnd
10.10.30.4  30.33.1.2  1480  30000  17998  17      683751850  471553      0x0
    0x0  0x90105c8  0x1a005000  14096494  14153835
30.33.1.2  10.10.39.4  4145  30000  18998  17      43858456  30164      0x0
    0x0  0x1a005000  0x1a006600  14096477  14099491
10.10.29.4  30.33.1.2  1479  30000  17998  17      683751850  471553      0x0
```

```

0x0 0x90105c7 0x1a005000 14096476 14153817
10.10.7.4 30.33.1.2 1457 30000 17998 17 683753300 471554 0x0
0x0 0x90105b1 0x1a005000 14096481 14153822
30.33.1.2 10.10.42.4 4145 30000 18998 17 95289344 65536 0x0
0x0 0x1a005000 0x1a006600 14112551 14119151
10.10.49.4 30.33.1.2 1499 30000 17998 17 683753300 471554 0x0
0x0 0x90105db 0x1a005000 14096486 14153827

```

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

```

