



NetFlow

A NetFlow system is a network traffic monitoring and reporting solution that

- identifies, classifies, and records packet flows traversing Nexus 9000 series switches,
- provides detailed flow-based statistics for IP and Layer 2 packet data, and
- supports advanced features for accounting, network performance, and security analysis without direct modification to network traffic or devices.

NetFlow does not require any change to the packets or to the networking device. 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. Cisco NX-OS can gather NetFlow statistics and analyze all packets on the interface or subinterface.

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) 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.

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 can create a flow using a flow record to define the unique keys for your flow. 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. The flow record determines the size of the data to be collected for a flow. Flows are stored in the NetFlow cache. The flow monitor combines the flow record and flow exporter with the NetFlow cache information.

- [NetFlow Fundamentals, on page 2](#)
- [Ingress NetFlow, on page 5](#)
- [Egress NetFlow, on page 12](#)
- [General Procedures to Enable NetFlow, on page 14](#)
- [Additional Procedures for Ingress NetFlow, on page 21](#)
- [Additional Procedures for Egress NetFlow, on page 24](#)
- [Drop Reports, on page 25](#)

NetFlow Fundamentals

Key Components

Table 1: Key Components of Netflow

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

Type	Definition
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.
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.

Type	Definition
NetFlow Output Interface	The NetFlow output interface on Cisco Nexus switches have the following features: • NetFlow in the show flow cache command displays <code>output_if_id</code> and exports output interface to the collector. • The NetFlow output interface for Cisco Nexus platform switches supports both IPv4 and IPv6 traffic flows. However, 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 <code>output_if_id</code> as 0x0. However, beginning with Cisco NX-OS Release 10.3(3)F, the show flow cache command displays <code>output_if_id</code> as 0x0 only if the destination IP address cannot be resolved or is not installed in the routing table or the packet received is control packet. • 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 <code>InputInt</code> and <code>OutputInt</code> support the full 32-bit SNMP <code>ifIndex</code> 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.

**Note**

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.

**Note**

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.

Architecture

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.

Types

From Cisco NX-OS Release 10.4(1)F, NetFlow consists of two types configurations:

Table 2: Types of Netflow

Type	Definition
Ingress Netflow	Ingress NetFlow identifies packet flows for ingress IP packets and provides statistics based on the packet flows. Ingress NetFlow uses flows to provide statistics for accounting, network monitoring, and network planning.
Egress Netflow	Egress NetFlow identifies packet flows for outgoing IP packets and Layer 2 flows and provides statistics based on these packet flows. On Cisco Nexus Cloudscale 9000 switches, egress NetFlow uses ingress pipeline and ingress TCAM carving egr-netflow to record flow information egressing out of the switch. All parameters and restrictions of NetFlow such as flow records, flow exporters, and flow monitors are applicable to egress NetFlow.

Ingress NetFlow

Guidelines and Limitations



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

General Limitations

- NetFlow is not supported on tunnel interfaces.
- NetFlow is not supported for CPU-transmitted packets.
- Flow collection is not performed for ARP traffic.
- 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.
- NetFlow is not supported on loopback and switch management interfaces.
-
- The Cisco Nexus 3232C and 3264Q switches do not support NetFlow.
- NetFlow for MPLS/VXLAN datapath is not supported
- 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.
- Flows are identified with Ingress(0) field in CFLOW packet.

ICMP and Non-TCP/UDP Flows

- On Nexus 9000 Switches, NetFlow collects ICMP flow information and sends it to the collector. ICMP type and code are inherently included in the packets. ICMP packets in NetFlow or flow export records do not use traditional source and destination ports like TCP or UDP. Instead, the exporter often encodes the ICMP type and code into fields like SPORT (source port) and DPORT (destination port). For example:
 - ICMP Echo Request: SPORT=2048, DPORT=0
 - ICMP Echo Reply: SPORT=0, DPORT=0
 - ICMP Time Exceeded: SPORT=2816, DPORT=0

Configuration and Operational Guidelines

- Flow cache can be cleared per flow type, such as Layer 2, IPv4, and IPv6. It cannot be cleared per flow monitor.
- 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 and Layer 3 Interface Limitations

- 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 vice versa, 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).
- VLAN and Layer 3 interfaces use different ACLs and must be treated as two different profiles.
- If you try to modify a record that is programmed in hardware during a rollback, the rollback fails.

Release Specific Guidelines

- *Cisco NX-OS Release 9.2(1)*
-

-
- *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.
- *Cisco NX-OS Release 9.3(1)*
 - Commands **record netflow ipv4 original-input**, **record netflow ipv4 original-output**, and **record netflow layer2-switched input** are not supported.
 - The NetFlow **output_if_id** is supported on 9300-FX switches.
- *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.
 - Ingress NetFlow is supported on Cisco Nexus 9300-GX platform switch.
 - The NetFlow **output_if_id** is supported on 9300-FX3 switches.
- *Cisco NX-OS Release 9.3(4)*
 - 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 9504, 9508, and 9516 with the 9736C-FX line card
- *Cisco NX-OS Release 10.1(2)*

- Netflow is supported on N9K-X9716D-GX line card.
- - 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.
- Ingress 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.
- *Cisco NX-OS Release 10.3(3)F*
 - Netflow Output_if_id is supported on Cisco Nexus 9300-FX2, 9300-GX, and 9300-GX2 switches and 9500-GX Line Cards.
 - For unicast flows, if the output_if_id is shown as 0x0, it means that the destination IP is not resolved or not available in the routing table or the ARP table.
 - The output_if_id is shown as 0x0 for received packets destined to the control-plane. Examples of such traffic are routing protocols or ICMP packets.
 - For IPv6 flows on Cisco Nexus 9500 Line Cards, output_if_id is shown as Unsupported due to hardware limitations.
 - The output_if_id for data plane multicast traffic will be shown as 0x0.
- *Cisco NX-OS Release 10.4(1)F*
 - Ingress NetFlow is supported on N9K-C9332D-H2R switch. Drop flows is not supported by default. To enable drop flows, configure the **hardware flow-table collect-drop-reason** command.
- *Cisco NX-OS Release 10.4(2)F*
 - The Ingress NetFlow for MPLS packet feature is supported on Cisco Nexus 9300-FX, 9300-FX2, 9300-FX3, 9300-GX, 9300-GX2, and 9500-FX/GX switches. This feature allows the Nexus switches to capture IPv4 or IPv6 flow information from MPLS packets and send the flow information to the collector. NetFlow captures information for packets with up to 8 MPLS stacked labels and supports capturing of MPLS packets such as IPoMPLS and EoMPLS packets and MPLS-VPN packets with two labels. The show flow cache shows output interface on MPLS-VPN encapsulation node as 0x0. The NetFlow output interface supports MPLS-VPN on transit or P nodes. This feature has the following limitations:
 - Due to the hardware ASIC limitations, NetFlow cannot capture MPLS related parameters such as MPLS label.
 - On transit or P nodes, MPLS VPNs with overlapping IP addresses with the same Layer 2 source and destination ports are reported as a single flow in the MPLS-VPN network.

- Ingress NetFlow is supported on N9K-C93400LD-H1 switch. Drop flows is not supported by default. To enable drop flows, configure the **hardware flow-table collect-drop-reason** command.

VXLAN Environment Limitations

- NetFlow for VXLAN traffic is supported including OIF (output interface). The feature nv overlay command must be enabled on the VXLAN transit node to capture inner flow details. If not, NetFlow captures only the outer header information.
- OIF on VXLAN Encapsulation node is shown as 0x0.
- 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.

Platform Limitations

- Ingress NetFlow is not supported on Cisco Nexus 92348GC-X platform switch.
- 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-FX
 - Cisco Nexus 9300-FX2
 - Cisco Nexus 9300-FX3
 - Cisco Nexus 9300-GX
 - Cisco Nexus 9500 with EX and FX line cards
- *Cisco Nexus 9300-FX Platform Switches*
 - NetFlow VLANs are supported for switched traffic only, and NetFlow SVIs are supported for routed traffic 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 is added.
- Cisco Nexus 9300-FX2 platform switches support sFlow and SPAN coexistence.
-
- 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. This applies to all Cisco Nexus 9500 platform switches with EX and FX line cards.

-
-

Prerequisites

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

Configure Ingress 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](#).
-

Configuration Example for Ingress NetFlow

This example shows how to configure an Ingress 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
```

Ingress NetFlow Verification Commands

An Ingress NetFlow verification command is a diagnostic command that

- displays the status and configuration of Ingress NetFlow features on a device,
- provides detailed information on flows, interfaces, exporters, and records, and

- helps administrators troubleshoot and validate NetFlow operations.

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

Command	Purpose
show flow cache [ipv4 ipv6 ce]	Displays information about Ingress NetFlow IP flows. Note This command can appear to be not valid on the EOR switches and no flows can be seen. To view this command on the EOR switches, attach to the module using the attach mod x command or check this command using the slot x quoted “ show flow cache ” command where x is the module number of the ingress NetFlow.
show flow exporter [name]	Displays information about Ingress 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 Ingress NetFlow interfaces.
show flow record [name]	Displays information about Ingress 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 Ingress NetFlow configuration.
show running-config netflow	Displays the NetFlow configuration that is currently on your device.

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 Ingress 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

Egress NetFlow

Guidelines and Limitations



Note For verified NetFlow scalability numbers, see [Cisco Nexus 9000 Series NX-OS Verified Scalability Guide](#).

- If both ingress and egress NetFlow are enabled on an interface, ingress NetFlow is prioritized over egress NetFlow and flow information is generated in ingress direction.
- Flows are identified with Egress(1) field in CFLOW packet.
- Egress NetFlow and feature analytics can coexist, but the traffic flows that hit analytics filters are only exported to collectors configured under analytics.
- On modular Cisco Nexus 9500 chassis, traffic comes in and goes out on different line cards. If egress NetFlow is enabled on traffic outgoing interface and not enabled on traffic incoming interface, the egress flow information is captured on ingress interface line card and not captured on egress interface.
- If there are more than one SVI and sub_interface on L2 interface, the ingress interface (if_id) derivation need not be correct for egress NetFlow.
- Egress NetFlow is supported only for IPv4 and Layer 2 traffic. Egress NetFlow does not support IPv6 and multicast traffic.
- Egress NetFlow does not support the following:
 - vrf-id
 - Recording of outgoing control plane traffic
 - Output Interface (NetFlow OIF)
 - MPLS network

Prerequisites

1. Configure the Nexus 9000 switches with egress NetFlow TCAM region.
2. Reload the switch after egress NetFlow TCAM carving.
3. When the switch comes online, enable the egress NetFlow on any L2 or L3 interface under interfaces using the **ip flow monitor <> output or layer2-switched flow monitor <> output** command.

Configure Egress NetFlow

Procedure

-
- Step 1** [Enable the NetFlow feature.](#)
- Step 2** Perform egr-netflow TCAM carving and reload the switch.
- a) **configure terminal**

Example:

```
switch# configure terminal
switch(config)#
```

Enters global configuration mode.
 - b) **[no] hardware access-list tcam region egr-netflow {0 | 512}**

Example:

```
switch(config)# hardware access-list tcam region egr-netflow 512
```

Enables egress NetFlow TCAM carving, and the default is disabled. The supported values are 0 and 512 for egr-netflow TCAM carving.
 - c) **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

Copies the running configuration to the startup configuration.
 - d) **reload**

Example:

```
switch(config)# reload
This command will reboot the system. (y/n)? [n] y
```

Reloads the switch.
- Step 3** [Define a flow record](#) by specifying keys and fields to the flow.
- Step 4** [Define a flow exporter](#) by specifying the export format, protocol, destination, and other parameters.
- Step 5** [Define a flow monitor](#) based on the flow record and flow exporter.
- Step 6** [Apply the flow monitor to a source interface](#), subinterface, or VLAN interface.
-

Configuration Example for Egress NetFlow

This example shows how to configure an egress 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 output
ip address 10.20.1.1/24
no shutdown

```

Egress NetFlow Verification Commands

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

Command	Purpose
show flow cache [ipv4 ce] [output]	Displays information about egress NetFlow IP flows.
show running-config netflow	Displays the egress NetFlow configuration that is currently on your device.

Display Example for Egress NetFlow

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

```

switch(config-if-range)# show flow cache
NOTE: Only 10k flows are displayed in XML output
Egress 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
Profile      Ing-VRF
130.1.1.2    162.1.1.1    4119     60        893        6         161082
171          0x0          0x0      0x1a002600 0x1a002800  716994    732532
      4 : NF    21
130.1.1.2    162.1.1.1    4151     60        11013      6         61230
65          0x0          0x0      0x1a006600 0x1a006800  715951    728074
      4 : NF    38
130.1.1.2    162.1.1.1    4145     60        3441       6         162966
173          0x0          0x0      0x1a005a00 0x1a005c00  713085    727941
      4 : NF    35

```

General Procedures to Enable NetFlow

The following sections list the procedures that are common to both Ingress and Egress NetFlow when you enable them.

Enable NetFlow feature

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.

Create 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: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	flow record <i>name</i> Example: <pre>switch(config)# flow record Test switch(config-flow-record)#</pre>	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: <pre>switch(config-flow-record)# description IPv4Flow</pre>	Describes this flow record as a maximum 63-character string.
Step 4	(Optional) match <i>type</i> Example:	Specifies a match key. For more information, see Specify match parameters, on page 16 .

Specify match parameters

	Command or Action	Purpose
	<code>switch(config-flow-record)# match transport destination-port</code>	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: <code>switch(config-flow-record)# collect counter packets</code>	Specifies the collection field. For more information, see Specify collect parameters, on page 17 .
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: <code>switch(config-flow-record)# show flow record netflow protocol-port</code>	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: <code>switch(config-flow-record)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

Specify 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: <code>switch(config-flow-record)# match datalink ethertype</code>	Specifies the Layer 2 attribute as a key.
match ip { protocol tos } Example: <code>switch(config-flow-record)# match ip protocol</code>	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.

Command	Purpose
match ipv4 {destination address source address} Example: <pre>switch(config-flow-record)# match ipv4 destination address</pre>	Specifies the IPv4 source or destination address as a key.
match ipv6 {destination address source address flow-label options} Example: <pre>switch(config-flow-record)# match ipv6 flow-label</pre>	Specifies the IPv6 key.
match transport {destination-port source-port} Example: <pre>switch(config-flow-record)# match transport destination-port</pre>	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.

Specify collect parameters

In Cisco/NX-OS NetFlow, “collect parameters” are the configuration options you specify within a flow record that indicate which fields or metrics are captured from a network flow for export and analysis.

You must configure at least one of the following collect parameters for the 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.

Command	Purpose
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.

Create 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 name 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 {ipv4-address ipv6-address} [use-vrf name] Example: <pre>switch(config-flow-exporter)# destination 192.0.2.1</pre>	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: <pre>switch(config-flow-exporter)# source ethernet 2/1</pre>	Specifies the interface to use to reach the NetFlow Collector at the configured destination.
Step 5	(Optional) description string Example: <pre>switch(config-flow-exporter)# description exportversion9</pre>	Describes this flow exporter. You can enter up to 63 alphanumeric characters for the description.
Step 6	(Optional) dscp value Example: <pre>switch(config-flow-exporter)# dscp 0</pre>	Specifies the differentiated services codepoint value. The range is from 0 to 63.
Step 7	(Optional) transport udp port Example: <pre>switch(config-flow-exporter)# transport udp 200</pre>	Specifies the UDP port to use to reach the NetFlow Collector. The range is from 0 to 65535. Note

	Command or Action	Purpose
		If you do not specify the UDP port, 9995 is selected as the default.
Step 8	version 9 Example: <pre>switch(config-flow-exporter)# version 9 switch(config-flow-exporter-version-9)#</pre>	Specifies the NetFlow export version. Choose version 9 to enter the flow exporter version 9 configuration submenu.
Step 9	(Optional) option {exporter-stats interface-table} timeout seconds Example: <pre>switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200</pre>	Sets the flow exporter statistics resend timer. The range is from 1 to 86400 seconds.
Step 10	(Optional) template data timeout seconds Example: <pre>switch(config-flow-exporter-version-9)# template data timeout 1200</pre>	Sets the template data resend timer. The range is from 1 to 86400 seconds.
Step 11	(Optional) copy running-config startup-config Example: <pre>switch(config-flow-exporter-version-9)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Create 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: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	flow monitor name Example: <pre>switch(config)# flow monitor flow-monitor-one switch(config-flow-monitor)#</pre>	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:	Describes this flow monitor. You can enter up to 63 alphanumeric characters for the description.

	Command or Action	Purpose
	<code>switch(config-flow-monitor)# description IPv4Monitor</code>	
Step 4	(Optional) exporter name Example: <code>switch(config-flow-monitor)# export v9</code>	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: <code>switch(config-flow-monitor)# record IPv4Flow</code>	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: <code>switch(config-flow-monitor)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

Apply Flow Monitor to an Interface

You can apply a flow monitor to an interface. You can apply a flow monitor in egress direction using the **output** keyword instead of **input**.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
Step 2	interface vlan vlan-id Example: <code>switch(config)# interface vlan 10</code> <code>switch(config-if)#</code>	Configures a VLAN interface and enters interface configuration mode.
Step 3	ip flow monitor {ipv4 ipv6 layer-2-switched} input Example: <code>switch(config-if)# ip flow monitor ipv4 input</code>	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:	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	<code>switch(config-if)# copy running-config startup-config</code>	

Additional Procedures for Ingress NetFlow

The following section lists the various other procedures you can apply to Ingress NetFlow.

Configure Bridged NetFlow on 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: <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
Step 2	vlan configuration <i>vlan-id</i> Example: <code>switch(config)# vlan configuration 30</code> <code>switch(config-vlan-config)#</code>	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 <i>name</i> Example: <code>switch(config-vlan-config)# ip flow monitor testmonitor</code>	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: <code>switch(config-vlan-config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

Configure 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: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	flow record <i>name</i> Example: <pre>switch(config)# flow record L2_record switch(config-flow-record)#</pre>	Enters flow record configuration mode. For more information about configuring flow records, see Create a flow record, on page 15 .
Step 3	match datalink {mac source-address mac destination-address ethertype vlan} Example: <pre>switch(config-flow-record)# match datalink ethertype</pre>	Specifies the Layer 2 attribute as a key.
Step 4	exit Example: <pre>switch(config-flow-record)# exit switch(config)#</pre>	Exits flow record configuration mode.
Step 5	interface {ethernet <i>slot/port</i> port-channel <i>number</i>} Example: <pre>switch(config)# interface Ethernet 6/3 switch(config-if#)</pre>	Enters interface configuration mode. The interface type can be a physical Ethernet port or a port channel.
Step 6	switchport Example: <pre>switch(config-if)# switchport</pre>	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: <pre>switch(config-if)# mac packet-classify</pre>	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: <pre>switch(config-if)# layer2-switched flow monitor L2_monitor input</pre>	Associates a flow monitor to the switch port input packets. You can enter up to 63 alphanumeric characters for the flow monitor name.

	Command or Action	Purpose
Step 9	(Optional) show flow record netflow layer2-switched input Example: <pre>switch(config-if)# show flow record netflow layer2-switched input</pre>	Displays information about the Layer 2 NetFlow default record.
Step 10	(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.

Configure 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: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	flow record name Example: <pre>switch(config)# flow record L3_record switch(config-flow-record)#</pre>	Enters flow record configuration mode. For more information about configuring flow records, see Create a flow record, on page 15 .
Step 3	interface {ethernet slot/port port-channel number} Example: <pre>switch(config)# interface Ethernet 6/3 switch(config-if#)</pre>	Enters interface configuration mode. The interface type can be a physical Ethernet port or a port channel.
Step 4	switchport Example: <pre>switch(config-if)# switchport</pre>	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 flow-name input Example: <pre>switch(config-if)# ip flow monitor v4l input</pre>	Associates an IPv4 flow monitor to the switch port input packets. You can enter up to 63 alphanumeric characters for the flow monitor name.

	Command or Action	Purpose
Step 6	ipv6 flow monitor <i>flow-name</i> input Example: switch(config-if)# ipv6 flow monitor v6l 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.

Configure 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.
Step 3	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Additional Procedures for Egress NetFlow

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:	Enters global configuration mode.

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
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 Create a flow record, on page 15 .
Step 3	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 4	switchport Example: switch(config-if)# switchport	Changes the interface to a Layer 2 mode. For information on configuring switch ports, see Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide .
Step 5	ip flow monitor <i>flow-name</i> input output Example: switch(config-if)# ip flow monitor v4l input switch(config-if)# layer2-switched flow monitor v4l output	or layer2-switched flow monitor <i>flow-name</i> input output Associates an IPv4 flow monitor to the switch port input or output packets. You can enter up to 63 alphanumeric characters for the flow monitor name.
Step 6	(Optional) copy running-config startup-config Example: switch(config-if)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Drop Reports

Beginning with Cisco NX-OS 10.5(2), users can utilize a new troubleshooting feature called the drop report. This can be used to help quickly narrow down troubleshooting like intermittent packet loss or congestion on single flow. This feature is supported on Cisco Nexus 9300- FX3/GX/GX2/HX platform switches. This feature supports the following drops:

- Policer Drops
- Forward Drops
- IDS Drops
- Buffer Drop
- RPF Drops

Guidelines and Limitations

This drop report has the following guidelines and limitations:

- Feature NetFlow is automatically enabled when users configure the drop report feature.
- A maximum of 10 flows matching the specified source and destination IPs are supported. To capture a different flow with specified source and destination IPs, the filter must be cleared and re-applied to restart report capturing.
- The drop report filter stays active for 10 minutes.
- The drop report feature is not supported if the feature analytics is already configured.
- Only single unique flow with 2-tuple(sip/dip) and best effort 5-tuple is supported at a time.
- This feature has no ISSU, ISSD, and reload support.

Configure Drop Report

You need to configure this feature by entering into the drop-report mode.

SUMMARY STEPS

1. **drop-report**
2. **start**
3. **filter {ipv4 [src-ip | dst-ip] | ipv6 [src-ip | dst-ip]}**
4. **report**
5. **clear**
6. **stop**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	drop-report Example: <pre>switch# drop-report switch(drop-report)#</pre>	Enters drop-report mode.
Step 2	start Example: <pre>sswitch(drop-report)# start Feature netflow enabled by drop report tool</pre>	Drop report enables feature NetFlow.
Step 3	filter {ipv4 [src-ip dst-ip] ipv6 [src-ip dst-ip]} Example: <pre>switch(drop-report)# filter ipv6 src-ip 100::1 dst-ip 200::2</pre>	Configures filter to assign parameters to the Access Control List (ACL).

	Command or Action	Purpose
	switch(drop-report)# filter ipv4 src-ip 192.168.1.2 dst-ip 192.168.1.1	
Step 4	report Example: switch(drop-report)# report	Shows drop information.
Step 5	clear Example: switch(drop-report)# clear CS drop filter removed	Removes ACL and stops recording.
Step 6	stop Example: switch(drop-report)# stop	Removes drop report feature.

Verify Drop Report Configuration

Use the following command to see the drop-report result:

For IPv4

```
switch# drop-report
switch(drop-report)# start
Feature netflow enabled by drop report tool
switch(drop-report)# filter ipv4 src-ip 10.0.0.9 dst-ip 10.0.0.10
switch(drop-report)# report
Filter Status: Applied    Filter Type   : IPv4
Dst IP: 10.0.0.10 Src IP: 10.0.0.9 Protocol: Dst Port: Src Port:
```

```
IPv4 Entries
SIP          DIP          BDId  SrcP  DstP  Prot  Byte Count  Packet Count
Ing Interface Fwd Rpf Pol Ids Acl Buf
10.0.0.9     10.0.0.10    4112  49280 3784  17    70          1
Ethernet1/8  0   0   0   0   0   0
```

Fwd: Forward Drop Rpf:RPF Fail Pol:Policer Drop Ids: Ids Drop Acl: Acl Drop Buf: Buffer Drop

For IPv6

```
switch(drop-report)# report
Filter Status: Applied    Filter Type   : IPv6
Dst IPv6: 2000:1::130:1:33:10 Src IPv6: 2000:1::22:1:1:10 Protocol: Dst Port: Src Port:
```

```
IPv6 Entries
SIP          DIP          BDId  SrcP  DstP  Prot  Byte Count  Packet Count
Ing Interface Fwd Rpf Pol Ids Acl Buf
2000:1::22:1:1:10 2000:1::130:1:33:10 4100  300  400  17    76494000    69540
Ethernet1/1      0   0   0   0   0   0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100  306  400  17    77632500    70575
Ethernet1/1      0   0   0   0   0   0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100  303  400  17    76320200    69382
```

Verify Drop Report Configuration

```

Ethernet1/1      0    0    0    0    0    0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 304  400  17  77745800      70678
Ethernet1/1      0    0    0    0    0    0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 308  400  17  77867900      70789
Ethernet1/1      0    0    0    0    0    0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 301  400  17  76458800      69508
Ethernet1/1      0    0    0    0    0    0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 307  400  17  77558800      70508
Ethernet1/1      1    0    0    1    1    0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 309  400  17  77943800      70858
Ethernet1/1      0    0    0    0    0    0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 302  400  17  76373000      69430
Ethernet1/1      0    0    0    0    0    0
2000:1::22:1:1:10 2000:1::130:1:33:10 4100 305  400  17  77706200      70642
Ethernet1/1      0    0    0    0    0    0

```

Fwd: Forward Drop Rpf:RPF Fail Pol:Policer Drop Ids: Ids Drop Acl: Acl Drop Buf: Buffer Drop

```

switch(drop-report)# clear
CS drop filter removed

```

```

switch(drop-report)# report
Filter Status: No Filter Applied

```