

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 13
- Sampled Netflow, on page 15
- General Procedures to Enable NetFlow, on page 17
- Additional Procedures for Ingress NetFlow, on page 24
- Additional Procedures for Egress NetFlow, on page 28
- Drop Reports, on page 29

• Dropped flow notification, on page 32

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 `output_if_id` 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 `output_if_id` as `0x0`. However, beginning with Cisco NX-OS Release 10.3(3)F, the **show flow cache** command displays `output_if_id` 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 `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.

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.
- Netflow and Flow Telemetry are not supported in N9K-C9364C-H1 platform SFP+ ports, Ethernet1/65, and Ethernet1/66.
- 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)*

- NetFlow for FEX Layer 3 ports is supported on Cisco Nexus 9300-FX platform switches.

- *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.
    - NetFlow does not export a flow record when the ingress and output interface IDs are the same. This behavior can reduce the number of exported records on a Layer 2 switch that is used for TAP aggregation.

      Use the show flow cache command to compare the if_id and output_if_id fields. If the fields are the same and these flows must be exported, disable MAC address learning globally by using the mac-learn disable command, and then clear dynamically learned MAC addresses by using the clear mac address-table dynamic command.

      For more information, see “Disabling MAC Address Learning on System” in the **Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide**.

- *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.

- *Cisco NX-OS Release 10.6(2)F*
  - Nexus 9300-SG2 switches support dropped flow notification feature.
  - Ingress NetFlow is supported on Nexus N9336C-SE1, N9396T12C-SE1, N9396Y12C-SE1, N9348Y12C-SE1, N9324C-SE1U, and N9348Y2C6D-SE1U switches.
  - Ingress NetFlow does not support hardware rate-limiter.
  - The show flow cache stores up to 1,000,000 flows. However, due to ASIC limitations, the byte count displayed in the output of this command is always zero (0) and the collector also receives a byte count of zero (0).
  - Output interfaces are not supported and are shown as 0x0 in the output of the show flow cache command.
  - The switches do not capture the control packets such as OSPF/BGP and self-IP packets such as BFD.
  - A single flow monitor cannot be used on Layer 3 and SVI interfaces simultaneously.
  - Up to 5 interface types are supported, and you can configure up to 14 profiles per interface type.
  - A Layer 3 flow monitor configured on Layer 3 interface cannot be applied to Layer 2 interfaces. Similarly, a Layer 2 flow monitor configured on Layer 2 interface cannot be applied to Layer 3 interfaces.
  - If a packet is denied by a Router Access Control List (RACL), the denied packet is still visible in the show flow cache records.
  - Ingress NetFlow allows 14 unique monitors to be active per acl key profiles. For ingress NetFlow there are 9 different acl key profiles pre-configured including all key types such as IPv4, IPv6 and MAC.

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.
- On Cisco Nexus 9300-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-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.
- 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.
- NetFlow is supported on Cisco Nexus 9500 platform switches with EX and FX mixed chassis. You can use SPAN simultaneously with NetFlow on the Cisco Nexus 9500 platform switches with EX and FX mixed chassis.
- 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 9500-EX platform switches.

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
- Beginning with Cisco NX-OS Release 10.6(2)F, Nexus 9300-SG2 switches support dropped flow notification feature.
- Beginning with NX-OS Release 10.6(2)F, although ingress NetFlow is supported on Nexus N9336C-SE1, N9396T12C-SE1, N9396Y12C-SE1, N9348Y12C-SE1, N9324C-SE1U, and N9348Y2C6D-SE1U switches, egress NetFlow is not supported on these switches.

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) Enter the global configuration mode using the command **configure terminal**

Example:

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

b) Enable egress NetFlow TCAM carving using the command [**no**] **hardware access-list tcam region egr-netflow** { **0** | **512** }

Example:

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

The default is disabled. The supported values are 0 and 512 for egr-netflow TCAM carving.

c) Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

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

d) Reload the switch using the command **reload**

Example:

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

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 a 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
```

Sampled Netflow

A sampled Netflow (SNF) is an analysis of NetFlow that

- enables sample-based traffic analysis with minimal performance impact,
- supports flexible and configurable sampling rates per flow monitor, and
- integrates seamlessly with existing NetFlow infrastructure and collectors.

NetFlow provides a comprehensive, high-accuracy view of all network conversations, ideal for deep security analysis, while sampled NetFlow gives a statistical overview of traffic, making it better for real-time monitoring of high-speed networks with minimal impact on the device performance.

Concept

Sampled NetFlow allows network administrators to sample and collect information about network traffic flows passing through the switch. SNF focuses on sampled (not all) traffic to reduce performance impact while still providing valuable insights. This sampled traffic data can then be sent to an external collector for analysis. For example, a network engineer can configure SNF to sample traffic on key ports, view flow records, and send this data to security tools to detect unusual patterns or attacks.

Sampled NetFlow uses a sampling mechanism similar to sFlow, using ASIC-level packet sampling. The sampling and export operations are hardware-assisted, ensuring minimal performance overhead. The NetFlow Manager (NFM) manages configuration, sampling rate, and export operations. The sampled NetFlow (SNF) feature provides packet-level traffic sampling for IPv4 and IPv6 flows, allowing administrators to collect representative network data at a configurable sampling rate. The sampled flow records are exported in NetFlow version 9 format for analysis, accounting, and traffic engineering.

Aspects

The three main aspects of SNF include :

- Flow configuration - As part of flow configuration, the focus is on sampling, that is, setting up of the traffic and ports to sample. SNF samples incoming traffic on both physical and logical switch ports and displays this information in tables. For more information, see **Create flow monitor**.
- Flow learning and collection handling - Gathering and managing the sampled traffic flow data is another aspect of SNF. The data is collected for both IPv4 and IPv6 flows. SNF supports flow record collection and formatting. Network administrators can use the information provided by SNF for tasks such as network management, planning, monitoring for security threats such as denial-of-service attacks, accounting, ISP billing, and data analysis.
- Flow export - SNF supports sending the collected data to external collectors for further use. You can export collected traffic flow data using NetFlow version 9 format. You can also export flow data to multiple external collectors at the same time.

Guidelines and Limitations

The guidelines and limitations for sampled NetFlow (SNF) configuration include:

General

- Beginning with 10.6.2(F), a new command is introduced under the existing flow monitor configuration to define the sampling rate.
- For VXLAN tunnel traffic, the outgoing interface is displayed as 0x0.

Supported features

- Sampled NetFlow is supported only on ingress NetFlow.
- Sampled NetFlow supports only two flow monitors at a time, for example, one IPv4 and one IPv6, two IPv4, or two IPv6 flow monitors. Note that the limitation is only on the number of monitors attached to interfaces. You can create more than two monitors but can attach only two of them at a time to interfaces.

- Each flow monitor supports two exporters.

Unsupported features

- sFlow and sampled NetFlow cannot co-exist due to shared session resource limits.
- SNF does not support egress sampled netflow, layer 2 interfaces, and CE monitor.

Hardware-rate limiter

- The default hardware-rate limiter for sampled NetFlow is 40000 pps. The supported range is 0-8,000,000. Use the show hardware rate-limiter netflow command to verify the hardware-rate limiter.

Platform support

- Beginning with 10.6(2)F, the sampled NetFlow feature is supported only on N9364E-SG2-O and N9364E-SG2-Q switches.

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 the NetFlow feature

Procedure

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

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

Step 2 Enable or disable the NetFlow feature using the command [**no**] **feature netflow**

Example:

```
switch(config)# feature netflow
```

The default is disabled.

Note
The Cisco Nexus 9500 platform switches with N9K-T2 EoR do not support NetFlow.

Step 3 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

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

This is an optional step.

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

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

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

Step 2 Create a flow record and enter flow record configuration mode using the command **flow record** *name*

Example:

```
switch(config)# flow record Test
 switch(config-flow-record)#
```

You can enter up to 63 alphanumeric characters for the flow record name.

Step 3 Describe this flow record as a maximum 63-character string using the command **description** *string*

Example:

```
switch(config-flow-record)# description IPv4Flow
```

This is an optional step.

Step 4 Specify a match key using the command **match** *type*

Example:

```
switch(config-flow-record)# match transport destination-port
```

This is an optional step. For more information, see Specify match parameters, on page 19 .

Note
The **match transport destination-port** and **match ip protocol** commands are required to export Layer 4 port data.

Step 5 Specify the collection field using the command **collect** *type*

Example:

```
switch(config-flow-record)# collect counter packets
```

This is an optional step. For more information, see Specify collect parameters, on page 20 .

Step 6 Display information about NetFlow flow records using the command **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
```

This is an optional step. You can enter up to 63 alphanumeric characters for the flow record name.

Step 7 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

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

This is an optional step.

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:** `switch(config-flow-record)# match datalink ethertype`	Specifies the Layer 2 attribute as a key.
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.

Command	Purpose
match transport {**destination-port** | **source-port**} **Example:** `switch(config-flow-record)# match transport destination-port`	Specifies the transport source or destination port as a key. **Note** The **match transport destination-port** and **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:** `switch(config-flow-record)# collect counter packets`	Collects either packet-based or byte counters from the flow. You can optionally specify that 64-bit counters are used.
collect 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.

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

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

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

Step 2 Create a flow exporter and enter flow exporter configuration mode using the command **flow exporter** *name*

Example:

```
switch(config)# flow exporter flow-exporter-one
  switch(config-flow-exporter)#
```

You can enter up to 63 alphanumeric characters for the flow exporter name.

Step 3 Set the destination IPv4 or IPv6 address for this flow exporter using the command **destination** { *ipv4-address* | *ipv6-address* } [**use-vrf** *name*]

Example:

```
switch(config-flow-exporter)# destination 192.0.2.1
```

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 Specify the interface to use to reach the NetFlow Collector at the configured destination using the command **source** *interface-type name/port*

Example:

```
switch(config-flow-exporter)# source ethernet 2/1
```

Step 5 Describe this flow exporter using the command **description** *string*

Example:

```
switch(config-flow-exporter)# description exportversion9
```

This is an optional step. You can enter up to 63 alphanumeric characters for the description.

Step 6 Specify the differentiated services codepoint value using the command **dscp** *value* and specify the UDP port to use to reach the NetFlow Collector using the command **transport udp** *port* .

Example:

```
switch(config-flow-exporter)# dscp 0
```

Example:

```
switch(config-flow-exporter)# transport udp 200
```

This is an optional step. The range for differentiated services coodepoint is from 0 to 63. The range for the UDP port is from 0 to 65535.

Note
If you do not specify the UDP port, 9995 is selected as the default.

Step 7 Specify the NetFlow export version using the command **version 9**

Example:

```
switch(config-flow-exporter)# version 9
 switch(config-flow-exporter-version-9)#
```

Choose version 9 to enter the flow exporter version 9 configuration submode.

Step 8 Set the flow exporter statistics resend timer using the command **option** { **exporter-stats** | **interface-table** } **timeout** *seconds*

Example:

```
switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200
```

This is an optional step. The range is from 1 to 86400 seconds.

Step 9 Set the template data resend timer using the command **template data timeout** *seconds* and copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

```
switch(config-flow-exporter-version-9)# template data timeout 1200
```

Example:

```
switch(config-flow-exporter-version-9)# copy running-config startup-config
```

This is an optional step. The range for the data resend timer is from 1 to 86400 seconds.

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

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

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

Step 2 Create a flow monitor and enter flow monitor configuration mode using the command **flow monitor***name*

Example:

```
switch(config)# flow monitor flow-monitor-one
 switch(config-flow-monitor)#
```

You can enter up to 63 alphanumeric characters for the flow monitor name.

Step 3 (Optional) Describe the flow monitor using the command **description***string*

Example:

```
switch(config-flow-monitor)# description IPv4Monitor
```

This is an optional step. You can enter up to 63 alphanumeric characters for the description.

Step 4 Associate a flow exporter with the flow monitor using the command **exporter***name*

Example:

```
switch(config-flow-monitor)# export v9
```

You can enter up to 63 alphanumeric characters for the exporter name.

Step 5 Associate a flow record with the specified flow monitor using the command **record***name* [**netflow-original** | **netflow protocol-port** | **netflow** { **ipv4** | **ipv6** } { **original-input** | **original-output** }]

Example:

```
switch(config-flow-monitor)# record IPv4Flow
```

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). These parameters are not supported on sampled NetFlow.

Step 6 Configure sampling rate using the command **sampling-rate**<*4096-1000000000*>

Example:

```
switch(config)# flow monitor myMonitor
switch(config-flow-monitor)# sampling-rate 5000
```

The default sampling rate is 4096.

Step 7 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

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

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

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

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

Step 2 Configure a VLAN interface and enter interface configuration mode using the command **interface vlan** *vlan-id*

Example:

```
switch(config)# interface vlan 10
  switch(config-if)#
```

Step 3 Associate an IPv4, IPv6, or Layer 2-switched flow monitor to the interface for input packets using the command **ip flow monitor** { **ipv4** | **ipv6** | **layer-2-switched** } **input**

Example:

```
switch(config-if)# ip flow monitor ipv4 input
```

Step 4 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

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

This is an optional step.

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

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

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

Step 2 Enter VLAN configuration mode using the command **vlan configuration** *vlan-id*

Example:

```
switch(config)# vlan configuration 30
  switch(config-vlan-config)#
```

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 Associate a flow monitor to the VLAN for input packets using the command { **ip** | **ipv6** } **flow monitor** *name*

Example:

```
switch(config-vlan-config)# ip flow monitor testmonitor
```

You can enter up to 63 alphanumeric characters for the flow monitor name.

Step 4 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

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

This is an optional step.

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

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

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

Step 2 Enter flow record configuration mode using the command **flow record** *name*

Example:

```
switch(config)# flow record L2_record
      switch(config-flow-record)#
```

For more information about configuring flow records, see Create a flow record, on page 18 .

Step 3 Specify the Layer 2 attribute as a key using the command **match datalink** { **mac source-address** | **mac destination-address** | **ethertype** | **vlan** }

Example:

```
switch(config-flow-record)# match datalink ethertype
```

Step 4 Exit flow record configuration mode using the command **exit** and enter interface configuration mode using the command **interface** { **ethernet** *slot/port* | **port-channel** *number* }

Example:

```
switch(config-flow-record)# exit
  switch(config)#
```

Example:

```
switch(config)# interface Ethernet 6/3
 switch(config-if#)
```

The interface type can be a physical Ethernet port or a port channel.

Step 5 Change the interface to a Layer 2 physical interface using the command **switchport**

Example:

```
switch(config-if)# switchport
```

For information on configuring switch ports, see the Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide .

Step 6 Force MAC classification of packets using the command **mac packet-classify**

Example:

```
switch(config-if)# mac packet-classify
```

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 7 Associate a flow monitor to the switch port input packets using the command **layer2-switched flow monitor** *flow-name* **input**

Example:

```
switch(config-if)# layer2-switched flow monitor L2_monitor input
```

You can enter up to 63 alphanumeric characters for the flow monitor name.

Step 8 Display information about the Layer 2 NetFlow default record using the command **show flow record netflow layer2-switched input**

Example:

```
switch(config-if)# show flow record netflow layer2-switched input
```

This is an optional step.

Step 9 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

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

This is an optional step.

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

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

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

Step 2 Enter flow record configuration mode using the command **flow record** *name*

Example:

```
switch(config)# flow record L3_record
 switch(config-flow-record)#
```

For more information about configuring flow records, see Create a flow record, on page 18 .

Step 3 Enter interface configuration mode using the command **interface** { **ethernet** *slot/port* | **port-channel** *number* }

Example:

```
switch(config)# interface Ethernet 6/3
  switch(config-if#)
```

The interface type can be a physical Ethernet port or a port channel.

Step 4 Change the interface to a Layer 2 mode using the command **switchport**

Example:

```
switch(config-if)# switchport
```

For information on configuring switch ports, see the Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide .

Step 5 Associate an IPv4 flow monitor to the switch port input packets using the command **ip flow monitor** *flow-name* **input**

Example:

```
switch(config-if)# ip flow monitor v41 input
```

You can enter up to 63 alphanumeric characters for the flow monitor name.

Step 6 Associate an IPv6 flow monitor to the switch port input packets using the command **ipv6 flow monitor** *flow-name* **input**

Example:

```
switch(config-if)# ipv6 flow monitor v61 input
```

You can enter up to 63 alphanumeric characters for the flow monitor name.

Step 7 Copy the running configuration to the startup configuration using the commnd **copy running-config startup-config**

Example:

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

This is an optional step.

Configure NetFlow Timeouts

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

Procedure

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

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

Step 2 Set the flush timeout value in seconds uisng the command **flow timeout** *seconds*

Example:

```
switch(config)# flow timeout 30
```

The range is from 5 to 60 seconds. The default value is 10 seconds.

Step 3 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

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

This is an optional step.

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

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

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

Step 2 Enter flow record configuration mode using the command **flow record** *name*

Example:

```
switch(config)# flow record L3_record
  switch(config-flow-record)#
```

For more information about configuring flow records, see Create a flow record, on page 18 .

Step 3 Enter interface configuration mode using the command **interface** { **ethernet** *slot/port* | **port-channel** *number* }

Example:

```
switch(config)# interface Ethernet 6/3
  switch(config-if#)
```

The interface type can be a physical Ethernet port or a port channel.

Step 4 Change the interface to a Layer 2 mode using the command **switchport**

Example:

```
switch(config-if)# switchport
```

For information on configuring switch ports, see Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide .

Step 5 Associate an IPv4 flow monitor to the switch port input or output packets using the commands **ip flow monitor** *flow-name* **input** | **output**

or

layer2-switched flow monitor *flow-name* **input** | **output**

Example:

```
switch(config-if)# ip flow monitor v41 input

switch(config-if)# layer2-switched flow monitor v41 output
```

You can enter up to 63 alphanumeric characters for the flow monitor name.

Step 6 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

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

This is an optional step.

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.

Procedure

Step 1 Enter drop-remote mode using the command **drop-report**

Example:

```
switch# drop-report
switch(drop-report)#
```

Step 2 Enable the NetFlow feature using the command **start**

Example:

```
sswitch(drop-report)# start
Feature netflow enabled by drop report tool
```

Step 3 Configure filter to assign parameters to the Access Control List (ACL) using the command **filter {ipv4 [src-ip | dst-ip] | ipv6 [src-ip | dst-ip]}**

Example:

```
switch(drop-report)# filter ipv6 src-ip 100::1 dst-ip 200::2
                      switch(drop-report)# filter ipv4 src-ip 192.168.1.2  dst-ip 192.168.1.1
```

Step 4 Shows drop information using the command **report**

Example:

```
switch(drop-report)# report
```

Step 5 Removes ACL and stop recording using the command **clear**

Example:

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

Step 6 Remove drop report feature using the command **stop**

Example:

```
switch(drop-report)# stop
```

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
      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
```

Dropped flow notification

Dropped flow notification is a feature that

- allows network administrators to capture packets that are otherwise dropped due to forwarding issues or insufficient buffer space in the queue,
- achieves this by copying the drop packets to CPU for the configured drop events, and
- exporting them to collector in version 9 format indicating the flow details and the reason for the drop, thus assisting in identifying the cause of packet loss.

Note

- The export limit based on the configurable timer is 64,000.
- The packets are rate limited to CPU so the dropped packet count is approximate.

Configure Dropped Flow Notification

Perform these steps to configure dropped flow notification.

Procedure

Step 1 Enable the NetFlow feature.

Step 2 Enable event export interval using the **flow event export-interval** <*interval*> command to specify the rate at which the data is exported. The range of export-interval is 0-60 seconds and default value is 10 seconds.

Example:

```
switch(config)# flow event export-interval 50
```

Step 3 Create a flow exporter.

Step 4 Configure a UDP port using the **events transport udp** <*udp-port*> command for exporting event data. The range of UDP port is 1-65535.

Example:

```
switch(config-flow-exporter)# events transport udp 9001
```

Step 5 Create a flow record.

Step 6 Create flow monitor.

Step 7 Configure events to be captured using the **flow event** <*event_name*> command.

Example:

```
switch(config-flow-monitor)# flow event ee
```

a) Use the **capture buffer-drops**, **capture fwd-drops**, **capture acl-drops**, or all three event configuration commands to define the packet drops that should be monitored.

Example:

```
switch(config-flow-event)# capture buffer-drops

switch(config-flow-event)# capture acl-drops

switch(config-flow-event)# capture fwd-drops
```

Step 8 Enter the **flow system config** command in global configuration mode to define system-level flow event settings.

Example:

```
switch(config-flow-event)# flow system config
```

a) Enter the **monitor** <*mon_name*> **input** command to associate an existing NetFlow monitor with the system's input traffic.

Example:

```
switch(config-flow-system)# monitor mon_ipv4 input
```

b) Enter the **event** <*event_name*> command to apply a pre-configured event definition to the system-wide flow event configuration.

Example:

```
switch(config-flow-system)# event ee
```

Sample configuration for dropped flow notification

Here is an example that displays the complete configuration for dropped flow notification.

```
switch(config)# feature netflow
switch(config)# flow event export-interval 50
switch(config)# flow exporter exp_2
switch(config-flow-exporter)# destination 50.50.50.53
switch(config-flow-exporter)# transport udp 9996
switch(config-flow-exporter)# source Ethernet1/7
switch(config-flow-exporter)# events transport udp 9001
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)# flow record rec_ipv4
switch(config-flow-record)# match ipv4 source address
switch(config-flow-record)# match ipv4 destination address
switch(config-flow-record)# match ip protocol
switch(config-flow-record)# match ip tos
switch(config-flow-record)# match transport source-port
switch(config-flow-record)# match transport destination-port
```

```
switch(config-flow-record)# flow monitor mon_ipv4
switch(config-flow-monitor)# record rec_ipv4
switch(config-flow-monitor)# exporter exp_2
switch(config-flow-monitor)# flow event ee
switch(config-flow-event)# capture buffer-drops
switch(config-flow-event)# capture acl-drops
switch(config-flow-event)# capture fwd-drops
switch(config-flow-event)# flow system config
switch(config-flow-system)# monitor mon_ipv4 input
switch(config-flow-system)# event ee
switch(config-flow-system)#
```

Verification commands for dropped flow notification

Based on your purpose, use the show commands for dropped flow notification configuration mentioned in the table.

Table 3: Verification commands for dropped flow notification

Command	Purpose
show flow event	Displays information about the drop events.
show flow event cache [**ipv4** | **ipv6**]	Displays information about dropped flows.
show flow system	Displays information about the system configuration.
show flow event export-interval	Displays the interval at which dropped flows are exported.