

Mixed Mode

This chapter describes how to configure the Mixed Mode (Analytics and NetFlow) feature on NX-OS devices.

This chapter contains the following sections:

- Mixed Mode, on page 1
- Guidelines and limitations for Mixed Mode, on page 1
- Mixed mode use cases, on page 2
- Commands for verifying the Mixed Mode configuration, on page 5
- Display example for Mixed Mode, on page 6

Mixed Mode

You can configure NetFlow and Analytics features on a switch, so both the features coexist and utilize the standard Version 9 export from the Central Processing Unit (CPU). This mode, in which both the features coexist, is called the Mixed Mode.

Note Until NX-OS Release 10.2(3)F, standard Version 9 export was supported only for NetFlow flow records. Beginning from NX-OS Release 10.2(3)F, standard Version 9 export is supported for Analytics also. However, NetFlow and Analytics features are mutually exclusive.

Guidelines and limitations for Mixed Mode

The guidelines and limitations applicable to Mixed Mode are:

- Beginning with NX-OS Release 10.3(1)F, both NetFlow and Analytics can co-exist and use the standard V9 export from CPU resulting in decreased processing load on the collectors. However, this mixed mode is not supported on 9300-EX modules. Furthermore, transition to mixed mode is not possible to or from Analytics mode. The applicable guidelines and limitations are as follows:
  - L2 flow monitor is not supported.
  - VRF filter is not supported.
  - ND ISSU is not supported.

  - The IPv4 and IPv6 profiles are as follows:
    - IP flow monitor: 28
    - IPv6 flow monitor: 26
  - Analytics record configuration must be a superset of all the record parameters.
  - Configure system monitor before configuring any system filter/interface filter configurations.
  - Unconfigure system filter/interface filter configurations, before unconfiguring system monitor.
  - In Mixed mode, two NetFlow records are exported for AN flow on EOR.
- Interface based FT is not supported for tunnel traffic flows such as MPLS, VXLAN, and GRE.
- Beginning with NX-OS Release 10.3(3)F, ingress_vrf_id is supported for the NetFlow and Analytics features on all Nexus 9000 switches.

  The ingress vrf-id is captured, shown in **show flow cache** and sent to NetFlow collector.

  When Layer 3 NetFlow is configured on a Layer 2 interface and the traffic is sent, and then the **show flow cache** command output displays the value of Ingress_VRF_ID as zero.
- Beginning with NX-OS Release 10.3(3)F, the NetFlow mixed mode is enabled by default. This reduces the TCAM space assigned to the Analytics feature from a maximum of 512 entries to a maximum of 256 entries.
- Beginning with NX-OS Release 10.3(3)F, flow record is seen when it is defined in system filter, but not defined in interface filter unlike in earlier releases. In the earlier releases, if the interface filter is configured, the flow record was seen only if it was defined in the interface filter.

Mixed mode use cases

The three possible use cases or scenarios for Mixed mode are:

- switches already deployed with feature analytics
- switches already deployed with feature netflow, and
- switches that have neither feature configured.

Mixed mode can be configured only from NetFlow mode. In a scenario where the switches already have feature analytics enabled, unconfigure analytics first, configure feature netflow, and then transition to Mixed mode.

After configuring the mixed mode, use the standard Version 9 format to export both NetFlow and Analytics flow records from the CPU to the respective collectors.



Note Analytics data is a superset of NetFlow data. The additional analytics flow data such as flow latency, traffic burst data, payload length, TCP flags, IP flags, and packet disposition flags is communicated through Vendor Specific Fields (VSF).

Switches already deployed with feature analytics

This section provides information for the use case or scenario where the switch is already deployed with feature analytics.

Unconfigure or save feature analytics configuration and perform the steps indicated in Switches that have neither features configured. Note that transition to Mixed mode is not possible to or from Analytics mode.

Switches already deployed with feature netflow

The steps mentioned in this use case is for switches that already have feature netflow deployed on them.

Procedure

Configure feature analytics based on this sample configuration.

Example:

```
feature analytics
           analytics
           flow filter telemetryFP
           ipv4 telemetryIpv4Acl
           ipv6 telemetryIpv6Acl
           flow exporter e11
           destination 10.10.20.21 v9
           transport udp 1100
           events transport udp 55
           source Ethernet1/42
           flow exporter e12
           destination 10.10.20.21 v9
           transport udp 9200
           events transport udp 555
           source Ethernet1/42
           flow record fte-record
           match ip source address
           match ip destination address
           match ip protocol
           match transport source-port
           match transport destination-port
           collect counter packets
           collect timestamp sys-uptime first
           collect timestamp sys-uptime last
           flow monitor m1
           record fte-record
           exporter-bucket-id 1 0 4095
           exporter e11
           flow monitor m2
           record fte-record
           exporter-bucket-id 1 0 2000
           exporter e11
           exporter-bucket-id 2 2001 4095
           exporter e12
           flow profile telemetryProf
           collect interval 1000
           source port 1001
           flow event fte-event1
           group drop-events
           capture buffer-drops
           capture acl-drops
```

```
capture fwd-drops
group packet-events
capture tos 50
capture ttl 50
flow system config
exporter-id 4
monitor m1 input
profile telemetryProf
event fte-event1
filter telemetryFP
```

Switches that have neither features configured

This use case is for switches that have neither NetFlow nor Analytics features configured.

Procedure

Configure feature netflow and then perform either the steps mentioned in Switches already deployed with feature NetFlow or from the sample configuration provided here.

Example:

```
feature netflow
        feature analytics
        flow exporter e1
        destination 10.10.20.21
        transport udp 100
        source Ethernet1/42
        version 9
        flow record r4
        match ipv4 source address
        match ipv4 destination address
        match ip protocol
        match transport source-port
        match transport destination-port
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
        flow record r6
        match ip protocol
        match transport source-port
        match transport destination-port
        match ipv6 source address
        match ipv6 destination address
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
        flow monitor m41
        record r4
        exporter e1
        flow monitor m6
        record r6
        exporter e1
        analytics
```

```
flow filter telemetryFP
ipv4 telemetryIpv4Acl
ipv6 telemetryIpv6Acl
flow exporter e11
destination 10.10.20.21 v9
transport udp 1100
events transport udp 55
source Ethernet1/42
flow exporter e12
destination 10.10.20.21 v9
transport udp 9200
events transport udp 555
source Ethernet1/42
flow record fte-record
match ip source address
match ip destination address
match ip protocol
match transport source-port
match transport destination-port
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
flow monitor m1
record fte-record
exporter-bucket-id 1 0 4095
exporter e11
flow monitor m2
record fte-record
exporter-bucket-id 1 0 2000
exporter e11
exporter-bucket-id 2 2001 4095
exporter e12
flow profile telemetryProf
collect interval 1000
source port 1001
flow event fte-event1
group drop-events
capture buffer-drops
capture acl-drops
capture fwd-drops
group packet-events
capture tos 50
capture ttl 50
flow system config
exporter-id 4
monitor m1 input
profile telemetryProf
event fte-event1
filter telemetryFP
interface Ethernet1/42
ip flow monitor m41 input
ipv6 flow monitor m6 input
```

Commands for verifying the Mixed Mode configuration

Use any of the show commands listed in the table to verify the required mixed mode configuration.

Command	Purpose
show flow cache [**ipv4** | **ipv6**]	Displays information about NetFlow IP flows. **Note** Beginning with NX-OS Release 10.3(3)F, this command output also displays Ingress VRF ID. The ingress vrf-id is captured, shown in show flow cache and sent to NetFlow collector.
show flow exporter [*name*]	Displays information about NetFlow and Analytics flow exporters and statistics. You can enter up to 63 alphanumeric characters for the flow exporter name.
show flow interface [*interface-type slot/port*]	Displays information about NetFlow and Analytics interfaces.
show flow record [*name*]	Displays information about NetFlow and Analytics flow records. You can enter up to 63 alphanumeric characters for the flow record name.
show running-config [**netflow** | **analytics**]	Displays the coexisting NetFlow and Analytics configuration that is currently on your device.
show flow monitor	Displays the NetFlow and Analytics monitor configuration.
show flow system	Displays information about the Analytics system configuration.
show flow filter	Displays information about Analytics filters.
show flow profile	Displays information about the Analytics profile.
show flow event	Displays information about the Analytics events.

Display example for Mixed Mode

This section provides sample outputs of the **show flow cache** command.

Note

- Only 10,000 flows are displayed in XML output.
- When Layer 3 NetFlow is configured on a Layer 2 interface and the traffic is sent, and then the **show flow cache** command is run, the output displays the value of Ing-VRF as zero.

show flow cache

```
Ingress IPV4 Entries
SIP             DIP          BD ID    S-Port   D-Port   Protocol  Byte Count   Packet Count
  TCP FLAGS    TOS     if_id       flowStart     flowEnd      Profile    Ing-VRF
```

```
192.0.2.2        192.0.2.1    1671     0        0        89        480          8
    0x0          0xc0     0x1a004400  2938966       2976728      5  : NF    0
192.0.2.2        224.0.0.13   1672     0        0        103       144          2
    0x0          0xc0     0x1a004400  2941719       2969951      5  : NF    0
192.0.2.2        224.0.0.13   1675     0        0        103       72           1
    0x0          0xc0     0x1a004400  2961417       2961667      5  : NF    0
192.0.2.2        224.0.0.5    1675     0        0        89        340          5
    0x0          0xc0     0x1a004400  2943341       2979400      5  : NF    0
192.0.2.2        192.0.2.1    1671     2048     0        1         3612         43
    0x0          0x0      0x1a004400  2938188       2980184      5  : NF    0

Ingress IPV6 Entries
SIP                         DIP       BD ID    S-Port  D-Port  Protocol  Byte Count Packet
 Count  TCP FLAGS Flow Label  if_id       flowStart  flowEnd    Ing-VRF
fe80::822d:bfff:fe81:e415   ff02::5   4147     0       0       89        490        5
        0x0       0x0         0x1a003400  11217548   11254367   1
```