

Configuring Mixed Mode

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

This chapter contains the following sections:

- About Mixed Mode, on page 1
- · Guidelines and Limitations for Mixed Mode, on page 1
- Mixed Mode: Use Cases, on page 2
- Verifying the Mixed Mode Configuration, on page 5
- Display Example for Mixed Mode, on page 6

About Mixed Mode

You can configure NetFlow and Analytics features on a switch, so both the features coexist and utilize the standard V9 export from CPU. This mode, in which both the features coexist, is called the mixed mode.



Note

Until Cisco NX-OS Release 10.2(3)F, standard V9 export was supported only for NetFlow flow records. Beginning from Cisco NX-OS Release 10.2(3)F, standard V9 export was supported for Analytics also. However, NetFlow and Analytics features were mutually exclusive.

Guidelines and Limitations for Mixed Mode

The following guidelines and limitations are applicable to Mixed mode:

- Beginning with Cisco 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 config must be a superset of all the record parameters.
- Configure system monitor before configuring any system filter/interface filter configs.
- Unconfigure system filter/interface filter configs, 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 Cisco NX-OS Release 10.3(3)F, Ingress_VRF_ID is supported for the NetFlow and Analytics features on all Cisco 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 Cisco 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 Cisco 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

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

The following are the possible use cases for mixed mode:

- Switches already deployed with feature Analytics
- · Switches already deployed with feature NetFlow
- Switches that have neither feature configured

After configuring the mixed mode, use the standard V9 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).

Use Case: Switches Already Deployed with Feature Analytics

Unconfigure or Save feature Analytics configuration and perform the steps indicated in Use Case: Switches that have Neither Features Configured. Note that transition to mixed mode is not possible to or from Analytics mode.

Use Case: Switches Already Deployed with Feature NetFlow

Perform the following procedure for switches that already have feature netflow deployed on them:

1. Use the following command to perform team carving for mixed mode:

hardware flow-table analytics-netflow



Note This command disrupts the flow monitoring and record exports for a brief period.

2. Configure feature analytics as follows:

```
feature analytics
analytics
  flow filter telemetryFP
   ipv4 telemetryIpv4Acl
   ipv6 telemetryIpv6Acl
  flow exporter ell
   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 ell
  flow monitor m2
   record fte-record
    exporter-bucket-id 1 0 2000
     exporter ell
    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
```

Use Case: Switches that have Neither Features Configured

Configure feature netflow and then perform either the steps mentioned in Use Case: Switches Already Deployed with Feature NetFlow or the following steps:

```
feature netflow
hardware flow-table analytics-netflow
feature analytics
flow exporter el
 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 el
flow monitor m6
  record r6
  exporter el
analytics
  flow filter telemetryFP
   ipv4 telemetryIpv4Acl
   ipv6 telemetryIpv6Acl
  flow exporter ell
   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
```

L

```
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 ell
 flow monitor m2
   record fte-record
   exporter-bucket-id 1 0 2000
     exporter ell
   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
```

Verifying the Mixed Mode Configuration

To display the mixed mode configuration, perform one of the following tasks:

Command	Purpose					
show flow cache [ipv4 ipv6]	Displays information about NetFlow IP flows.					
	Note	Beginning with Cisco 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.				

Command	Purpose
show flow exporter [name]	Displays information about NetFlow/Analytics flow exporters and statistics. You can enter up to 63 alphanumeric characters for the flow exporter name.
show flow interface [<i>interface-type slot/port</i>]	Displays information about NetFlow/Analytics interfaces.
show flow record [name]	Displays information about NetFlow/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/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

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



Note

• Only 10k flows are displayed in XML output.



Note 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	Protoc	col B	yte Co	unt Pack	et Count
TCP FLAGS	TOS	if_id	flowStart	flowE	Ind	Prof	ile	Ing-VRF	
17.1.1.2	17.1.1.	.1 1671	0	0	89		480	8	
0x0	0xc0	0x1a004400	2938966	297	76728	5	: NF	0	
17.1.1.2	224.0.0	0.13 1672	0	0	103		144	2	
0x0	0xc0	0x1a004400	2941719	296	59951	5	: NF	0	
17.1.1.2	224.0.0	0.13 1675	0	0	103		72	1	
0x0	0xc0	0x1a004400	2961417	296	51667	5	: NF	0	
17.1.1.2	224.0.0	0.5 1675	0	0	89		340	5	

0x0	0xc0 0	x1a004400	2943341	2	979400	5	: NF	0		
17.1.1.2	17.1.1.1	1671	2048	0	1		3612		43	
0x0	0x0 0	x1a004400	2938188	2	980184	5	: NF	0		
Ingress IPV6 Er	ntries									
SIP		DIP	BD ID	S-Por	t D-Port	Pro	tocol	Byte	Count	Packet
Count TCP FLA	AGS Flow Lab	el if id	flow	vStart	flowEnd	In	g-VRF			
fe80::822d:bfff	f:fe81:e415	ff02 :: 5	4147	0	0	89		490		5
0x0	0x0	0x1a00	3400 1121	L7548	11254367	1				

I