

Configuring sFlow

This chapter describes how to configure sFlow on Cisco IOS XR devices.

- sFlow Agent, on page 1
- Guidelines and Limitations for sFlow, on page 3
- Default Settings for sFlow, on page 4
- Configuring sFlow, on page 4
- Discard Codes on sFlow, on page 8

sFlow Agent

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
Sampled Flow	Release 7.5.1	Sampled flow (sFlow) allows you to monitor real-time traffic in data networks that contain switches and routers. It uses the sampling mechanism in the sFlow agent software on routers to monitor traffic and to forward the sample data to the central data collector. sFlow uses version 5 export format to forward sampled data.

Feature Name	Release Information	Feature Description
sFlow Enhancements	Release 7.3.4	With this release, the following enhancements are available with sFlow: • Discard codes 0, 1, 256, 257, and 258 are supported. This alerts the user about the packets dropped in the network. • Syslog notifications for flow monitor buffer and ring buffer status.
sFlow Enhancements	Release 7.3.3	With this release, the following enhancements are available with sFlow: • Maximum configurable sFlow datagram size allowed is greater than 1500B and up to 9KB. This allows for improved data processing by enabling the data packets to capture more network information. • Support for tunnel encapsulation, which allows for the secure movement of data from one network to the other. • Locally destined packets are now reported by sFlow output interface as format-0, value=0x3FFFFFF. This helps the users to identify the packet flows. The following new options are added to the **sflow options** command: • extended-ipv4-tunnel-egress • extended-ipv6-tunnel-egress

The sFlow Agent periodically polls the interface counters that are associated with a data source of the sampled packets. The data source can be an Ethernet interface, an EtherChannel interface, or a range of Ethernet

interfaces. The sFlow Agent queries the Ethernet port manager for the respective EtherChannel membership information and also receives notifications from the Ethernet port manager for membership changes.

When you enable sFlow sampling, based on the sampling rate and the hardware internal random number, the ingress and egress packets are sent to the CPU as an sFlow-sampled packet. The sFlow Agent processes the sampled packets and sends an sFlow datagram to the central data collector. In addition to the original sampled packet, an sFlow datagram includes the information about the ingress port, egress port, and the original packet length. An sFlow datagram can have multiple sFlow samples such as mix of flow samples and counter samples.

You can export input and ouput interface handles if the ingress or egress interface is a bundle or a BVI type. The exported interface handles are of the physical interfaces on which the packet arrived or departed and not the bundle or BVI itself.

Guidelines and Limitations for sFlow

Consider these points before configuring sFlow:

- Ingress sFlow is supported on Cisco NCS 5500 Series Routers on the line cards .
- Supports a maximum of eight export IPv4 and IPv6 destinations
- sFlow supports a maximum of two sampler maps.
- Supported sampling rate is 1 out of 262144 (maximum)
- Supports L3 Interface, L3 Bundle Interface, L3 subinterface, and L3 Bundle subinterface
- Does not support tunnel and PW-Ether interfaces.
- Supports up to 2000 L3 interfaces
- sFlow doesn't sample ARP, multicast, broadcast, and IP-in-IP packets.
- sFlow on bundle having members on different LCs have flows exported with the same ifindex id (of bundle interface, if I/O ifindex physical is not configured), but with different sub-agent id and sequence number.
- When native mode is enabled, the sFlow monitor does not export the extended router and gateway structures format check fields for MPLS traffic with IPv6 Explicit-Null labels

System Log Messages on sFlow

- The FLOW_SAMPLES_DROPPED syslog message alerts the user when the ring buffer is full. The ring buffer receives the sampled flow from the hardware process before exporting it to the sFlow collector where the analyzer tool extracts sFlow datagram.

  The following example shows the syslog message when ring buffer is full:

```
LC/0/2/CPU0:May 12 12:47:28.500 UTC: nfsvr[145]: %MGBL-FLOW-6-INFO_FLOW_SAMPLES_DROPPED
 : Flow samples for Netflow or SFlow from flow producer process got dropped in the input
 queue of the flow server process. Cumulative drop count is 98724. Possible reasons
include a high sampling rate or an increase in the traffic rate. These drops could be
transient.
```

  The ring buffer automatically returns to normal when traffic rate in the network reduces.

  The following example shows the syslog message when ring buffer returns to normal:

```
LC/0/2/CPU0:May 12 16:05:15.221 UTC: nfsvr[145]:
%MGBL-FLOW-6-INFO_FLOW_SAMPLES_DROPPING_STOPPED : Dropping of Netflow or sFlow samples
 in the input queue of flow server process has not happened for 10 minutes and operation
 is stable now. This is informational, no action required.
```

- The BUFFER_EXCEEDED syslog message alerts the user when the flow monitor buffer is full with the sampled flow.

  The following example shows the syslog message when flow monitor buffer is full:

  ```
  LC/0/11/CPU0:Dec 10 14:27:58.922 UTC: nfsvr[248]: %MGBL-SFLOW-6-INFO_BUFFER_SIZE_EXCEEDED
   : Buffer space of 256000 entries for monitor slow_mon has been exceeded. Possible
  reasons include low export rate limit and/or high sampling rate. This could be a transient
   issue too.
  ```

  The flow monitor buffer automatically returns to normal when traffic rate in the network reduces.

  The following example shows the syslog message when flow monitor buffer returns to normal:

  ```
  LC/0/11/CPU0:Dec 10 14:37:58.902 UTC: nfsvr[248]:
  %MGBL-SFLOW-6-INFO_BUFFER_EXCEEDING_STOPPED : Buffer space of 256000 entries for monitor
   slow_mon has not been exceeded for the last 10 minutes and is stable now. This is
  infomational, no action required.
  ```

Default Settings for sFlow

Here are the default sFlow parameters:

Table 2: Default Parameters for sFlow

Parameters	Default
sFlow sampling-rate	1 out of 10000 packets
sFlow sampling-size	128 bytes. The maximum configurable value for sampler size is 200 bytes.
sFlow counter-poll-interval	20 seconds
sFlow collector-port	6343

Configuring sFlow

Configuring sFlow includes:

- Configuring Exporter Map
- Configuring Monitor Map
- Configuring Sampler Map
- Configuring sFlow on an Interface
- Enabling sFlow on a Line Card

Configuring Exporter Map

This sample exporter map includes two exporter maps for IPv4 and IPv6 traffic. sFlow uses default collector-port number 6343.

Also, in the below sample configuration the DF-bit (Don't Fragment bit) is enabled for IPv4 header. However, the DF-bit configuration is not supported for IPv6 transport.



Note A DF bit is a bit within the IP header that determines whether a router is allowed to fragment a packet.

```
flow exporter-map SF-EXP-MAP-1
 version sflow v5
 !
 packet-length 1468
 transport udp 6343
 source GigabitEthernet0/0/0/1

 source-address 192.127.10.1

 destination 192.127.0.1
 dfbit set
!

flow exporter-map SF-EXP-MAP-2
 version sflow v5
 !
 packet-length 1468
 transport udp 6343
 source GigabitEthernet0/0/0/1

 source-address db8::1

destination  FF01::1
!
```

Configuring Monitor Map

This sample monitor map records sFlow traffic. Optionally, you can choose to include extended router and extended gateway information in the monitor map.

The extended router information includes:

- nexthop
- source mask length
- destination mask length

The extended gateway information includes:

- nexthop
- communities
- local preference
- AS, source AS, source peer AS, and desgtination AS path

```
flow monitor-map sflow-mon1
 record sflow
 sflow options
  input ifindex physical
  output ifindex physical
  if-counters polling-interval 10
  extended-router
  extended-gateway
 !
 exporter sflow-exp-v6-0012_99992
 cache entries 5000
 cache timeout active 5
 cache timeout inactive 10
!
```

Verification

```
show flow monitor-map sflow-mon1
Thu Nov 11 10:47:48.015 IST

Flow Monitor Map : sflow-mon1
-----------------------------------------------
Id:                 6
RecordMapName:      sflow (1 labels)
ExportMapName:      sflow-exp-v4-0012_30001
                    sflow-exp-v6-0012_99992
CacheAgingMode:     Normal
CacheMaxEntries:    5000
CacheActiveTout:    5 seconds
CacheInactiveTout: 10 seconds
CacheUpdateTout:    N/A
CacheRateLimit:     2000
HwCacheExists:      False
HwCacheInactTout:   50

sFlow options:
  Option: extended router
  Option: extended gateway
  Option: Input ifindex physical
  Option: Output ifindex physical
  Option: Max sample header size: using default: 128
```

Configuring Sampler Map

This sample configuration samples 1 out of 20000 packets:

Note The default sampling rate is 10000.

```
sampler-map SF-SAMP-MAP
 random 1 out-of 20000
!
```

Verification

```
Flow Exporter Map : sflow-exp-v6-0012_99992
-----------------------------------------------
Id                  : 26
```

```
Packet-Length       : 1500
DestinationIpAddr   :
VRFName             : default
SourceIfName        : Loopback0
SourceIpAddr        : ::10:0:0:3
DSCP                : 45
TransportProtocol   : UDP
TransportDestPort   : 6402
Do Not Fragment     : Enabled

Export Version: sFlow Protocol
sFlow protocol version: v5
```

Configuring sFlow on an Interface

In the following example, sFlow configuration is applied on an interface at the ingress direction:

```
interface GigabitEthernet0/0/0/3
 ipv4 address 192.127.0.56 255.255.255.0
 ipv6 address FFF2:8:DE::56/64
 ipv6 enable
 flow datalinkframesection monitor-map SF-MON-MAP sampler SF-SAMP-MAP ingress
```

Enabling sFlow on a Line Card

This sample configuration enables sFlow on a line card at node 0/0/CPU0:

```
Router(config)# hw-module profile netflow sflow-enable location 0/0/CPU0
```

You should reload the line card for the changes to take effect.

Verify sFlow Configuration

Exporter Map

To verify if the exporter map has sFlow v5 export version configured, use the **show flow monitor-map** command:

```
Router# show flow monitor-map sflow-mon1

Flow Monitor Map : sflow-mon1
-----------------------------------------------
Id:                6
RecordMapName:     sflow (1 labels)
ExportMapName:     sflow-exp-v4-0012_30001
                   sflow-exp-v6-0012_99992
CacheAgingMode:    Normal
CacheMaxEntries:   5000
CacheActiveTout:   5 seconds
CacheInactiveTout: 10 seconds
CacheUpdateTout:   N/A
CacheRateLimit:    2000
HwCacheExists:     False
HwCacheInactTout:  50

sFlow options:
  Option: extended router
  Option: extended gateway
  Option: Input ifindex physical
```

```
  Option: Output ifindex physical
  Option: Max sample header size: using default: 128
```

Exporter Statistics Information

To view the flow, counter samples, and packet exported statistics, use the **show flow monitor sflow-mon1 cache location** command:

```
Router#show flow exporter SF-EXP-MAP-1 location 0/RP0/CPU0
show flow monitor sflow-mon1 cache location 0/0/cPU0
Thu Nov 11 10:57:35.168 IST
Cache summary for Flow Monitor sflow-mon1:
Cache size:                             5000
Current entries:                           0
Flows added:                          326328
Flows not added:                           0
Ager Polls:                            44656
  - Active timeout                         0
  - Inactive timeout                       0
  - Immediate                         326328
  - TCP FIN flag                           0
  - Emergency aged                         0
  - Counter wrap aged                      0
  - Total                             326328
Periodic export:
  - Counter wrap                           0
  - TCP FIN flag                           0
Flows exported                        326328
sFlow details:
  - flow samples:                     299639
  - counter samples:                   26689
     0 (0 bytes)
```

Discard Codes on sFlow

The sFlow discard code notifies the user about the packets that are dropped in the network. You can extract the discard codes from the sFlow packets using a flow-analyzer tool.

The following table lists supported discard codes on sFlow:

Table 3: Discard Codes on sFlow

Discard Code	Drop Reason	Description
0	Net unreachable	Packets dropped due to the network being unreachable
1	Host unreachable	Packets dropped due to incomplete adjacency
256	Unknown	Packets dropped due to unknown reason
257	Bad TTL	Packets dropped due to bad TTL

Discard Code	Drop Reason	Description
258	ACL Deny	Packets dropped due to denied ingress ACL