sFlow Configuration for Traffic Monitoring and Analysis

This page helps you with information about the key concepts, advantages and limitations of sFlow, and steps to configure sFlow on your router.

- sFlow Essential Concepts and Terms, on page 1
- Flow monitoring on Egress Interface, on page 2
- How sFlow Works, on page 2
- sFlow Parameters and Default Values, on page 5
- sFlow Sampling, on page 5
- Configure sFlow, on page 6

sFlow Essential Concepts and Terms

This section helps you get familiar with the sFlow key terms and concepts:

- **Data source:** Location within a network device that can make traffic measurements. Examples are physical interfaces, VLANs.
- **Flow**: A Flow is defined as a set of IP packets passing a network device in the network during a certain time interval. All packets that belong to a particular Flow have a set of common properties derived from the data contained in the packet.
- **Flow record**: A Flow record is a set of key and non-key sFlow field values used to characterize flows. This record is created by inspecting packet headers and adding a description of packet information.
- **sFlow agent:** Entity inside the network device responsible for maintaining sFlow configuration, gathering the sampled flow and counters from one or more data sources in the router, packaging them in sFlow datagram format, and exporting them to the sFlow collector.
- **sFlow collector:** Application that receives the sFlow datagrams from one or more agents to perform further analysis and generate reports. The collector is external to the router.
- **Sampling rate:** Frequency that specifies how often packet sampling is performed, and determines how many packets (on average) that pass through the data source to generate a flow sample. A value of 100 means that on average, 1 out of 100 packets is randomly sampled to be exported.
- **Sampling interval:** Period at which counters will be polled for populating the counter sample in the sFlow datagram.

- **sFlow datagram:** User Datagram Protocol (UDP) datagram exported from sFlow agent to collector. The datagram contains information about the data source, one or more flow samples, and one or more counter samples.
- **Collector address:** IP and UDP port number. The default destination port number is 6343.

Flow monitoring on Egress Interface

Egress Interface Flow Monitoring enhances network visibility and control by prioritizing outbound traffic. This capability offers advanced monitoring and management of data exiting the network, providing a more comprehensive understanding of network dynamics. The key focus of this feature is to monitor packets that are either encapsulated or decapsulated through egress sFlow.

Encapsulated and decapsulated data monitoring in sFlow serves a crucial role in safeguarding sensitive information transmitted across the network. The process involves encapsulating data with an additional layer of information, enabling verification of its authenticity and integrity. This added layer makes it challenging for attackers to intercept or modify data during transmission. Conversely, decapsulation entails removing the encapsulated data layer, empowering network devices to analyze the information and take appropriate actions in real-time. This proactive approach aids in identifying and preventing attacks or anomalies, enhancing the overall security of the network.

How sFlow Works

sFlow, a monitoring technology, operates by sampling data network traffic in real-time. However, it's important to note that sFlow doesn't encompass all network traffic, unlike Netflow.

In the context of traffic monitoring, sFlow functions by disaggregating the flow pipeline. Devices within the network stream packet headers and metadata, which are subsequently transmitted as UDP datagrams to an external collector. This collector deciphers the packets and creates flow records. A notable feature of sFlow is its capability to export this data promptly, facilitating the creation of a near real-time representation of network traffic by the collector.

The advantage of this real-time traffic analysis is its ability monitor patterns and trends within the network, facilitate the automation of traffic engineering, and aid in making well-informed decisions when planning network capacity.

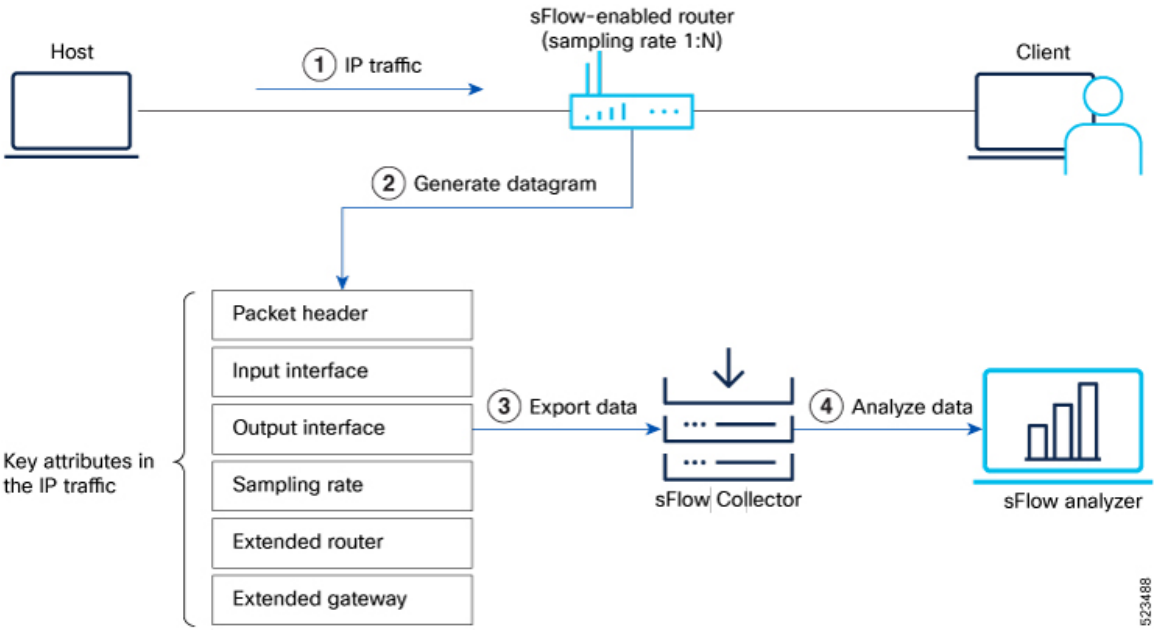
Table 1: Feature History Table

Feature Name	Release Introduced	Description
System Alerts Related to sFlow	Release 7.5.3	The following syslog notifications are available with sFlow: • FLOW_SAMPLES_DROPPED - This alert is seen whenever the buffer becomes full with sampled flow data, either due to a high sampling rate or an increase in the traffic rate. • FLOW_SAMPLES_DROPPING_STOPPED - This alert is seen when the buffer reverts to its regular state. • BUFFER_SIZE_EXCEEDED - This alert signals that the flow monitor buffer has reached its capacity with sampled flow data, which could be a result of a low export rate limit or a high sampling rate. • BUFFER_EXCEEDING_STOPPED - This alert is seen when the flow monitor buffer reverts to its regular state.
Ingress sFlow Enhancements	Release 7.3.3	The incoming sFlow packet offers the following enhancements to improve scalability and decrease the volume of packets received: • Expansion of sFlow datagram size—from 1500B to 9KB • Tunnel encapsulation—The packet header now supports an extended structure encompassing tunnel header information. The egress packet extracts the tunnel information during decapsulation. • sFlow collector indicates discarded packets and locally targeted packets at the output interfaces, in a specific format along with drop value.
sFlow for L2 Interfaces	Release 7.3.1	Ingress sFlow on an L2 interface is introduced. Support for sFlow existed in earlier releases.
Sampled Flow	Release 7.2.12	Sampled flow (sFlow) allows you to monitor real-time traffic in data networks. It uses sampling mechanism in the sFlow agent software to monitor traffic and to forward the sample data to the central data collector.

Recording of Packet Flows in sFlow

The packet in sFlow is recorded as follows:

Figure 1: Packet Flows in sFlow



In sFlow, the focus is on collecting sampled network traffic data rather than recording full packet flows. sFlow is designed to provide a statistical overview of network traffic by sampling packets and extracting relevant information for analysis.

Here's how sFlow handles the recording of packet flows:

1. Sampling: sFlow agent process in network devices sample packets based on a configured sampling rate. The sampling rate determines the percentage of packets that will be selected for analysis. For example, a sampling rate of 1-in-100 means that 1% of the packets will be sampled.
2. Datagram Generation: The sFlow agent generates datagrams that contain information about the sampled packets. These datagrams include details such as packet header, sampling rate, port numbers, protocol information, and various flow statistics.
3. Data Export: The sFlow datagrams are periodically exported from the sFlow agent to a designated sFlow collector or analyzer. The export can be done using protocols like UDP or TCP, and the datagrams are typically sent in a structured format like XDR.
4. Analysis and Reporting: Upon receiving the sFlow data, the sFlow collector or analyzer processes and analyzes the information. It aggregates the sampled data to provide statistical insights into network traffic, including top talkers, protocol distribution, traffic patterns, and other metrics.

sFlow Parameters and Default Values

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
Increased sFlow Sample-Header Size	Release 7.3.4	You can now increase the sFlow sampling size to 343 bytes of the incoming or outgoing packet header. This enhancement lets the router export a larger sample to the flow-analyzer tool, enabling the tool to provide more accurate network analytics. In earlier releases, you could configure up to 200 bytes.

The following table lists the sFlow parameters and default values that you can use when configuring sFlow on the router:

Table 3: sFlow Parameters and Default Values

Parameter	Value	Command
Sampling rate	Default value: 1 out of 10000 packets	**sampler-map**
Sample header size	128 - 343 bytes (from Cisco IOS XR Release 7.3.4 onwards) 128 - 200 bytes (prior to Cisco IOS XR Release 7.3.4) Default value: 128 bytes	**flow monitor-map**
Counter poll interval	5-1800 seconds Default value: None	**flow monitor-map**
Collector port	Configurable. Default value: 6343	**flow exporter-map**

sFlow Sampling

The following methods are used in sFlow for capturing and analyzing network traffic:

- **Counter Sampling:** In the counter sampling method, only specific counters or statistics are sampled and collected for analysis. Instead of capturing and analyzing packets or flows, counter sampling focuses on monitoring and collecting information about specific network metrics or performance indicators. These metrics can include interface utilization, packet drops, CPU usage, memory usage, and other relevant statistics. Counter sampling provides a high-level view of network health and performance without the need to capture and analyze every single packet.
- **Flow Sampling:** Flow sampling, on the other hand, involves capturing and analyzing sampled network flows. A flow can be defined as a sequence of packets that share common attributes, such as source and destination IP addresses, port numbers, and protocol information. Flow sampling selects a subset of these flows for analysis. By capturing and analyzing flows, you can gain insights into traffic patterns, detect

anomalies, and monitor performance. Flow sampling allows for more granular analysis of network traffic compared to counter sampling.

You can choose the method depending on the specific monitoring needs and objectives of the network.

Configure sFlow

This page explains how to configure sFlow for monitor network traffic using sampled data.

sFlow Guidelines and Limitations

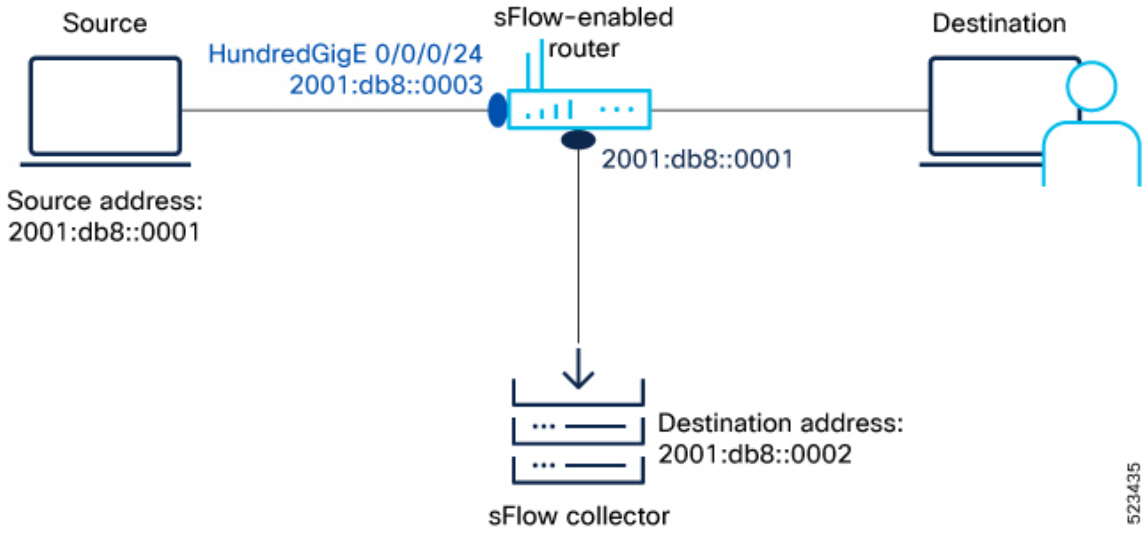
The guidelines and limitations of using flow samples and interface counters using sFlow monitoring is as follows:

- When you enable egress sFlow, the L2 information of ingress packets is captured instead of egress interface
- When sFlow is on a bundle with members located on different Line Cards (LCs), flows are exported with the same `ifindex` id for the bundle interface. However, they possess distinct sub-agent ids and sequence numbers
- sFlow samples are combined into UDP packets and forwarded to sFlow collectors for analysis. It's important to note that UDP, being a connectionless protocol, doesn't ensure the delivery of data. Consequently, utilizing sFlow as a flow source could potentially lead to inaccurate representations of traffic volumes, bidirectional flows, and a reduction in alerting capabilities
- Ingress sFlow is supported on Cisco 8200 and Cisco 8800 Series Routers
- Egress sFlow is supported only on Cisco 8200 Series Routers
- A maximum of 8 export destinations per monitor map for both IPv4 and IPv6 are allowed
- Only one sampler configuration per router is allowed
- A sampling interval of 1 out of 262,144 packets as the maximum is supported
- L3 interfaces, L3 bundle interfaces, L3 sub-interfaces, L3 bundle sub-interfaces, and L3 BVI interfaces are supported
- Up to 2000 L3 interfaces are supported
- Tunnel and Ethernet PseudoWire (PW) interfaces are not supported
- ARP, multicast, broadcast, and IP-in-IP packets are excluded from the sampling process

Configuring sFlow

To enable this monitoring, it is necessary to configure the sFlow agent to use a sampling mechanism, forwarding traffic data from both ingress and egress ports to a centralized data collector, also referred to as the sFlow analyzer. The sampled data is forwarded using the version 5 export format. You'll find instructions for configuring sFlow on the router in the following section. Let's use the following topology as a reference for configuring sFlow.

Figure 2: sFlow Configuration



Step 1 First, let's gather the required details to enable sFlow on a router:

- The IP address of the source : `2001:db8::0001`
- The IP address of the sFlow Collector (Destination address): `2001:db8::0002`
- Interface of the router where we will enable sFlow: `HundredGigE 0/0/0/24`
- sFlow version used to transport the data to the collector: `version 5`

Step 2 Configure the Flow Exporter using the flow flow exporter-map command to specify where and how the packets should be exported.

The following attributes can be configured while creating exporter map:

- Export destination IP address (IPv4 or IPv6 address). The same packets can be exported to multiple IPv4 or IPv6 destinations.
- DSCP value
- Source interface and its IP address
- Transport protocol
- UDP port number, where the collector listens to the packets
- Maximum datagram length
- Don't Fragment bit (DF-bit). The DF-bit within the IP header is supported only on IPv4 transport and determines whether the router is allowed to fragment a packet.

In this example, you create an exporter map called `EXP-MAP` to export the IPv4 packets to the destination address 192.127.10.1 using the UDP transport protocol:

```
Router(config)#flow exporter-map EXP-MAP
Router(config-fem)#version sflow v5
```

```
Router(config-fem)#packet-length 9000
Router(config-fem)#transport udp 6343
Router(config-fem)#source HundredGigE 0/0/0/1
Router(config-fem)#source-address 192.127.10.1
Router(config-fem)#destination 192.127.0.1
Router(config-fem)#dfbit set
```

Verify the Flow Exporter configuration using the show flow exporter-map command.

```
Router#show flow exporter-map EXP-MAP
Flow Exporter Map : EXP-MAP
------------------------------------------------
Id                    : 1
Packet-Length         : 9000
DestinationIpAddr     : 192.127.0.1
VRFName               : default
SourceIfName          : HundredGigE 0/0/0/3
SourceIpAddr          : 192.127.10.1
DSCP                  : 0
TransportProtocol     : UDP
TransportDestPort     : 6343

Export Version        : sFlow v5
```

The `Export Version: sFlow v5` indicates that the exporter map configuration is successful.

Step 3 Configure the Flow Sampler using sampler-map command to define the sampling rate for flow samples, which determines how many packets (on average) that pass through the data source will generate a flow sample.

In this example, you create a sampler map called `SAMP-MAP` to sample 1 out of every 4096 packets.

```
Router(config)#sampler-map SAMP-MAP
Router(config-sm)#random 1 out-of 4096
```

Verify the sampler map configuration using the show sampler-map command.

```
Router#show sampler-map SAMP-MAP
Sampler Map : SAMP-MAP
-----------------------------------------------
Id:         1
Mode:       Random (1 out of 4096 Pkts)
```

In this example, the sampler map configuration is successful with a sample rate of 1 out of every 4096 packets.

Step 4 Configure the Flow Monitor using flow monitor-map command to define the type of traffic to be monitored and the polling frequency. You can include one or more exporter maps in the monitor map.

In this example, you create a monitor map called `MON-MAP` and include the exporter map `EXP-MAP` to record sFlow data at a polling interval of 120 seconds:

```
Router(config)#flow monitor-map MON-MAP
Router(config-fmm)#record sflow
Router(config-fmm)#sflow options
Router(config-fmm-sflow)#extended-router
Router(config-fmm-sflow)#extended-gateway
Router(config-fmm-sflow)#if-counters polling-interval 120
Router(config-fmm-sflow)#input ifindex physical
Router(config-fmm-sflow)#output ifindex physical
Router(config-fmm-sflow)#sample-header size 200
Router(config-fmm-sflow)#exporter EXP-MAP
```

You can export input and ouput interface handles if the ingress or egress interface is a bundle or a Bridge-Group Virtual Interface (BVI).

Verify the monitor map configuration using the show sampler-map command.

```
Router#show flow monitor-map MON-MAP

Flow Monitor Map : MON-MAP
-----------------------------------------------
Id:                2
RecordMapName:     sflow
ExportMapName:     EXP-MAP
ExtendedRouter:    Enabled
ExtendedGateway:   Enabled
InterfaceCounters: Enabled
PollingInterval:   30 seconds
SampledHeaderSize: 200

Input ifhandle physical
Output ifhandle physical
```

In this example, the monitor map is configured successfully with the associated exporter map to monitor the interface counters at a polling interval of 30 seconds.

Step 5 Apply sFlow on an interface using command in Global Configuration mode.

In this example, you apply the monitor map `MON-MAP` and the sampler map `SAMP-MAP` on the HundredGigE 0/0/0/3 interface in the ingress direction to monitor the incoming packets:

```
Router(config)#interface HundredGigE 0/0/0/3
Router(config)#ipv4 address 192.127.0.56 255.255.255.0
Router(config)#ipv6 address FFF2:8:DE::56/64
Router(config)#flow datalinkframesection monitor-map MON-MAP sampler SAMP-MAP ingress
```

Step 6 Enable sFlow on the RP (0/RP0/CPU0) or on the line card using hw-module profile netflow sflow-enable command.

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

Step 7 Reload the line card using **hw-module reset auto** command.

```
Router#reload location 0/0/CPU0
```

With this configuration, sFlow is enabled on the line card.

Step 8 Verify the statistics of exported traffic flow at the producer and exporter using show flow platform producer statistics location and show flow exportercommands.

Producer:

```
Router#show flow platform producer statistics location 0/0/CPU0
Netflow Platform Producer Counters:
IPv4 Ingress Packets:                      0
IPv4 Egress Packets:                       0
IPv6 Ingress Packets:                      0
IPv6 Egress Packets:                       0
MPLS Ingress Packets:                      0
MPLS Egress Packets:                       0
IPFIX315 Ingress Packets:                  0
IPFIX315 Egress Packets:                   0
sFlow Ingress Samples:                100000
Drops (no space):                          0
Drops (other):                             0
Unknown Ingress Packets:                   0
Unknown Egress Packets:                    0
Worker waiting:                            0
```

Exporter:

```
Router#show flow exporter EXP-MAP location 0/0/CPU0
Wed June 21 04:21:36.263 UTC
```

```
Flow Exporter: EXP-MAP
Export Protocol: sFlow v5
Flow Exporter memory usage: 5247776
Used by flow monitors: MON-MAP

Status: Normal
Transport:   UDP
Destination: 192.127.0.1     (6343) VRF default
Source:      192.127.10.1    (6331)
Flows exported:                                50245 (9631004 bytes)
Flows dropped:                                     0 (0 bytes)

Packets exported:                               7372 (19262008 bytes)
Packets dropped:                                   0 (0 bytes)

Total export over last interval of:
  1 hour:                                       7363 pkts
                                              9629960 bytes
                                                50236 flows
  1 minute:                                       12 pkts
                                                1392 bytes
                                                  12 flows
  1 second:                                        0 pkts
                                                   0 bytes
                                                   0 flows
```

The sFlow configuration with flow and packet data is successful on the router.

What to do next

Analyze the traffic using the UDP datagram and sampled data collected at the sFlow collector.

This image shows an example of sampled data that has been collected at the sFlow collector.