Contents

1 Configuring sFlow

1.1 Introduction

1.1.1 Overview

Sampled flow (sFlow) is a network monitoring technology based on message sampling. It is mainly used for traffic statistics analysis when the network traffic is huge.

sFlow has the following advantages:

- Accurate: sFlow supports accurate monitoring of traffic on a Gigabit network or a network with higher bandwidth.
- Scalable: One sFlow Collector can monitor thousands of sFlow Agents, and it has high scalability.
- Low cost: sFlow Agent is embedded in a network device, and its cost is low.

1.1.2 Principles

The sFlow system consists of an sFlow Agent embedded in a device and a remote sFlow Collector. The sFlow Agent obtains interface statistics and data from the network device by using specific sampling technologies, encapsulates the information into sFlow packets, and sends them to the sFlow Collector. The sFlow Collector analyzes sFlow packets and displays the analysis results.

- **sFlow Agent**

  An sFlow Agent is embedded in a network device. Generally, one network device serves as an sFlow Agent.

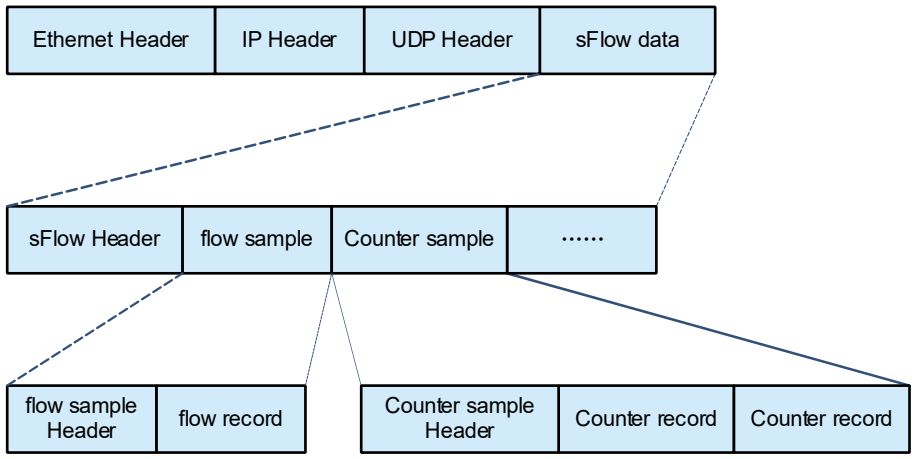
- **sFlow Collector**

  An sFlow Collector can be a PC or server that receives and analyzes sFlow packets from the sFlow Agent. A PC or server installed with the software used for sFlow packet analysis can be regarded as an sFlow Collector.

  The sFlow Agent performs flow sampling and counter sampling, encapsulates sampled data into sFlow packets, and sends them to the sFlow Collector.

  sFlow packets are encapsulated in UDP. Figure 1-1 shows the sFlow packet format.

Figure 1-1sFlow Packet Format



Note

One sFlow packet may contain one or more flow samples and counter samples.

Figure 1-2sFlow Header

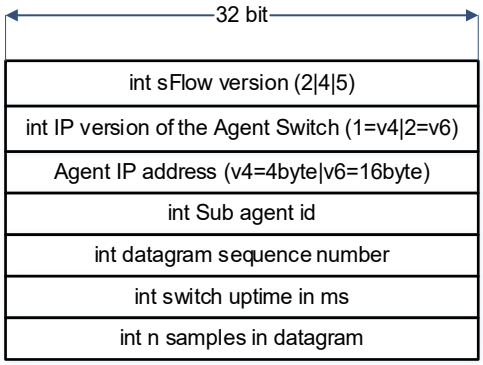


Table 1-1sFlow Header Description

Field	Description
sFlow version	sFlow version. V2, V4, and V5 are available. Currently, Orion supports V5 only.
IP version of the agent/switch	IP address version of the sFlow Agent
Agent IP address	IP address of the sFlow Agent
Sub agent id	Sub agent ID
Datagram sequence number	Serial number of an sFlow packet
Switch uptime	Duration from device startup to the current time

Field	Description
n samples in datagram	Number of samples in an sFlow packet. One sFlow packet contains one or more flow samples and counter samples.

1. Flow sampling

Based on the sampling rate configured for the specified interface, the sFlow Agent device performs flow sampling on packets through this interface, including copying the packet header, extracting the Ethernet header and IP header of each packet, and obtaining the route information of each packet. Then, the sFlow Agent encapsulates the flow sampling result into sFlow packets and sends them to the sFlow Collector for analysis.

Table 1-2Description of Fields in the Flow Record Part of the sFlow Packet

Field	Description
Raw packet	All or part of the header of the original packet (the extracted length depends on the configuration) is extracted and encapsulated into an sFlow packet and then sent to the Collector.
Extended Switch Data	For an Ethernet packet, the Ethernet header is parsed and encapsulated into an sFlow packet and then sent to the Collector.
Extended VNI Data	VNI ID of a VXLAN packet

2. Counter sampling

In counter sampling, the sFlow Agent periodically obtains the statistics and CPU usage from a specified interface. The sFlow Agent periodically performs interface polling, obtains the statistics from an interface where the counter sampling timer expires, encapsulates the statistics into an sFlow packet, and sends it to the sFlow Collector for analysis.

Table 1-1Description of Fields in the Counter Sampling Result

Field	Description
Generic Interface Counters	General interface statistics, including basic interface information and general interface traffic statistics
Ethernet Interface Counters	Ethernet-related traffic statistics of an Ethernet interface

1.1.3 Protocols and Standards

- sFlow Version 5: sFlow V5
- RFC 1014: XDR: External Data Representation standard

1.2 Configuration Task Summary

sFlow configuration includes the following tasks:

(1) Configuring Basic Functions of sFlow

(2) (Optional) Configuring Optional Parameters of sFlow

1.3 Configuring sFlow

1.3.1 Configuring Basic Functions of sFlow

1. Overview

- sFlow Agent and sFlow Collector can communicate with each other.
- Traffic flowing through the interface are sampled based on the default sampling rate and sent to the sFlow Collector for analysis.
- Statistics of the interface are periodically sent to the sFlow Collector based on the default sampling interval for analysis.

2. Restrictions and Guidelines

- The forwarding performance of an interface may be affected after flow sampling is enabled.
- To enable the sFlow Collector to analyze the flow sampling results, you must configure the IP address of the sFlow Collector on the sFlow Agent device.
- The sFlow Agent address must be a valid address. That is, the sFlow Agent address cannot be a multicast or broadcast address. It is recommended that the IP address of the sFlow Agent device be used.
- When the **vrf** parameter is configured, the corresponding VRF instance must exist. If you configure a VRF instance for an sFlow Collector address and later remove this VRF instance, the sFlow Collector address will be removed as well.
- You can enable flow sampling on a physical or an aggregation port.
- **sflow enable**
  - This command can be configured on a physical or an aggregation port.
  - If the direction is not specified, flow sampling is enabled in both the inbound and outbound directions.
  - Counter sampling is enabled when flow sampling is enabled in any direction of an interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the sFlow Agent address.

sflow agent { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **interface** [**ipv6**] *interface-type interface-number* }

No sFlow Agent address is configured by default.

(4) Configure the sFlow Collector address.

sflow collector *collector-id* **destination** { *ipv4-address* | **ipv6** *ipv6-address* } *udp-port-number* [**vrf** *vrf-name*] [**description** *collector-description*]

No sFlow Collector address is configured by default.

(5) Configure the ID of the sFlow Collector for flow sampling.

sflow flow collector *collector-id*

No ID of the sFlow Collector is configured for flow sampling by default.

(6) Configure the ID of the sFlow Collector for counter sampling.

sflow counter collector *collector-id*

No ID of the sFlow Collector is configured for counter sampling by default.

(7) Enable the counter sampling and flow sampling functions.

sflow enable [{ **ingress** | **egress** }

The sFlow function is disabled by default.

1.3.2 Configuring Optional Parameters of sFlow

1. Overview

You can adjust the data sampling accuracy by modifying relevant parameter attributes of sFlow.

2. Restrictions and Guidelines

- You can run the **sflow collector** command to configure the payload size of an sFlow packet, excluding the Ethernet header, IP header, and UDP header. One or more flow samples and counter samples can be encapsulated to an sFlow packet. When the maximum sFlow packet size is configured, different numbers of sFlow packets may be output after the same number of flow samples or counter samples are processed. If the maximum size is greater than MTU, the output sFlow packet is segmented.
- The **sflow sampling-rate** command is used to configure the global flow sampling rate. This configuration applies to all interfaces. The flow sampling rate may affect the sFlow sampling accuracy. A lower sampling rate indicates a higher accuracy and a larger CPU consumption, which may affect the forwarding performance of the interface.
- You can run the **sflow flow max-header** command to modify the configuration of packets sent to the sFlow Collector. For example, if you are concerned about the IP header, set the length to 56 bytes. During flow sampling, the first 56 bytes of a sample packet are encapsulated to the sFlow packet.
- This command is used to configure the maximum number of bytes that can be copied from the header of the original packet. The copied content is recorded in the generated sample. The protocol requires byte alignment during packet encapsulation, that is, the actual length of a sent packet is a multiple of 4. Therefore, the length of a collected packet may exceed the configured length. For example, when the maximum length is set to any of 21, 22, 23, and 24, the actual output packet length is 24.
- The **sflow counter interval** command is used to configure the global sFlow counter sampling interval. This configuration applies to all interfaces.
- The **sflow source** command is used to configure the source IP address of output packets. The default source address of output sFlow packets is the local device IP address which is used to ping the destination IP address. If the source interface is specified, the primary address (or the first global IPv6 address if any)

of the interface is the source IP address of output packets. If the source interface is not specified, the default source address is used.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum size of the output sFlow packet.

sflow collector *collector-id* **max-datagram-size** *datagram-size*

By default, the maximum size of the output sFlow packet is **1400**.

(4) Configure the sFlow flow sampling rate.

sflow sampling-rate *sampling-rate*

The default sFlow flow sampling rate is **8192**.

(5) Configure the maximum length of the packet header copied during flow sampling.

sflow flow max-header *sampling-length*

By default, the maximum length of the packet header copied during sFlow flow sampling is **64**.

(6) Configure the sampling interval.

sflow counter interval *sampling-interval-time*

The interface where counter sampling is enabled sends the interface statistics to the sFlow Collector at the sampling interval.

(7) Configure the source address of output sFlow packets.

sflow source { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **interface** [**ipv6**] *interface-type interface-number* }

By default, the source address of output sFlow packets is the local device IP address which is used to ping the destination IP address.

1.4 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Table 1-1sFlow monitoring

Command	Purpose
show sflow	Displays the sFlow configuration.
show sflow capacity	Display the sFlow capacity supported by the device.

1.5 Configuration Examples

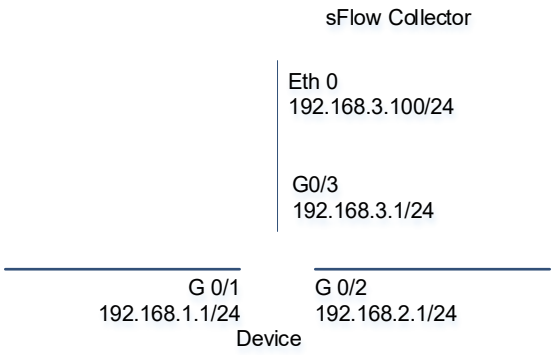
1.5.1 Configuring Basic Functions of sFlow

1. Requirements

Start the device that serves as the sFlow Agent, enable flow sampling and counter sampling on port G 0/1, monitor the traffic in the 192.168.1.0 network segment, encapsulate the sampling result into sFlow packets at regular intervals or when the buffer is full, and send these packets to the sFlow Collector for traffic analysis.

2. Topology

Figure 1-1Topology for sFlow Basic Functions



3. Notes

- Configure the L3 network reachable between the sFlow Agent and the sFlow Collector.
- Configure the sFlow function.

4. Procedure

Configure the L3 network reachable between the sFlow Agent and the sFlow Collector.

```
Device> enable
Device#configure terminal
Device(config)# interface GigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
Device(config)# interface GigabitEthernet 0/2
Device(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0
Device(config)# interface GigabitEthernet 0/3
Device(config-if-GigabitEthernet 0/1)# ip address 192.168.3.1 255.255.255.0
```

Configure 192.168.1.1 as the sFlow Agent address.

```
Device(config)# sflow agent address 192.168.1.1
```

Configure 192.168.3.100 as the address of sFlow Collector 1, and 6343 as the port number.

```
Device(config)# sflow collector 1 destination 192.168.3.100 6343
```

Configure the interface GigabitEthernet 0/1 to output flow samples and counter samples to sFlow Collector 1, and enable sFlow sampling on this interface.

```
Device(config)# interface GigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# sflow flow collector 1
Device(config-if-GigabitEthernet 0/1)# sflow counter collector 1
Device(config-if-GigabitEthernet 0/1)# sflow enable
```

5. Verification

Run the **show sflow** command to check whether the command output is consistent with the configuration.

```
Device# show sflow
sFlow datagram version 5
Global information:
Agent IP: 192.168.1.1
sflow counter interval:30
sflow flow max-header:64
sflow sampling-rate:8192
Collector information:
ID   IP                              Port Size VPN
1    192.168.3.100                   6343 1400
2    NULL                            0    1400
Port information
Interface                       CID  FID  Enable
TenGigabitEthernet 0/1          1    1    B
```

Figure 1-1 shows the Top N tab of sFlowTrend, which displays the flow sampling result and the source IP addresses with the Top 5 traffic. The inbound traffic 450 kpps, and the outbound traffic is also 450 kpps, which is consistent with the actual traffic.

Figure 1-2 is the Counters tab of sFlowTrend, which displays the counter sampling result. The inbound traffic is 450 kpps, and the outbound traffic is also 450 kpps. All packets are unicast packets.

Figure 1-1Flow Sampling Results

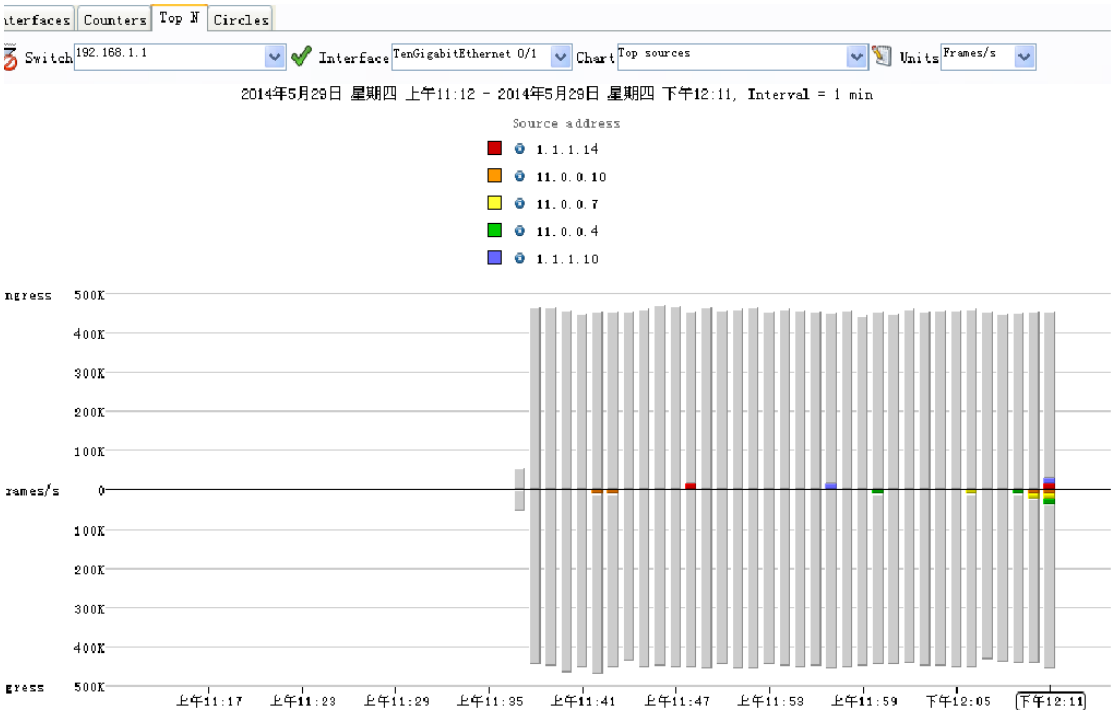
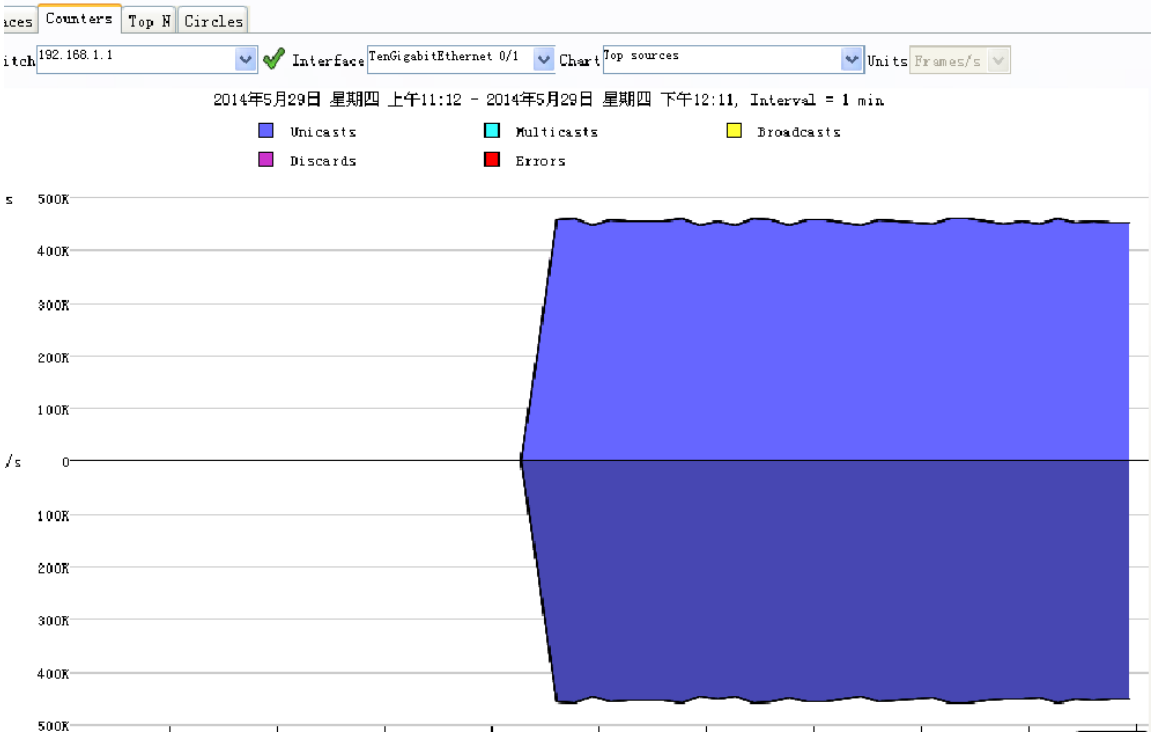


Figure 1-2Counter Sampling Results



6. Configuration Files

Device configuration file

```
Hostname Device
!
sflow agent address 192.168.1.1
sflow collector 1 destination 192.168.3.100 6343
!
interface GigabitEthernet 0/1
 ip address 192.168.1.1 255.255.255.0
 sflow counter collector 1
 sflow flow collector 1
 sflow enable
!
interface GigabitEthernet 0/2
 ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet 0/3
 ip address 192.168.3.1 255.255.255.0
!
end
```