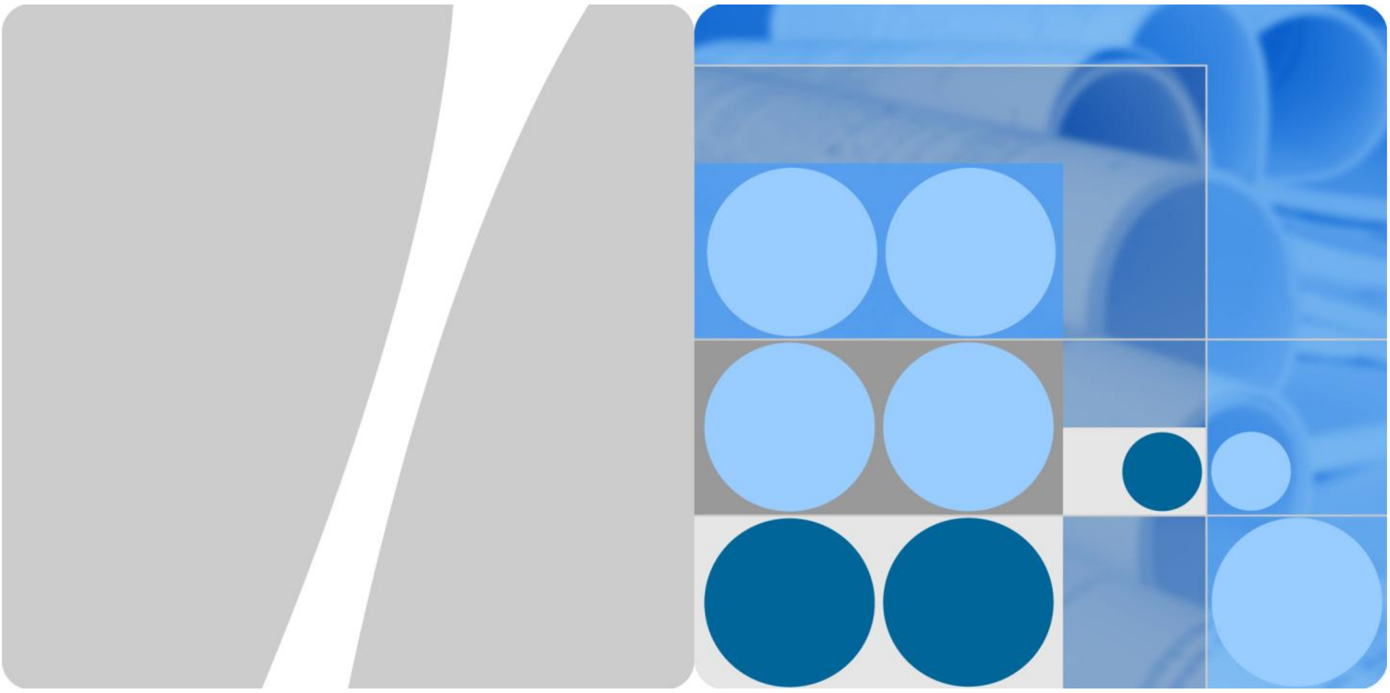


sFlow Technology White Paper

Issue 01

Date 2012-10-30

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2012. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Contents

Copyright © Huawei Technologies Co., Ltd.

sFlow

About This Chapter

1.1 Introduction

Definition

Sampled Flow (sFlow) is a traffic monitoring technology that collects and analyzes traffic statistics.

Purpose

Compared with carrier networks, enterprise networks have a smaller scale, provide flexible networking, and are prone to attacks. Due to these characteristics, enterprise networks often encounter service exceptions. Enterprises require a traffic monitoring technique on interfaces of devices to locate unexpected traffic and the source of attack traffic in a timely manner so that they can quickly rectify faults to ensure stable running of the network.

sFlow is developed to achieve the preceding purpose. sFlow is an interface-based traffic analysis technology that collects packets on an interface based on the sampling ratio. In flow sampling, an sFlow agent analyzes the packets including the packet content and forwarding rule, and encapsulates the original packets and parsing result into sFlow packets. Then the sFlow agent sends the sFlow packets to an sFlow collector. In counter sampling, an sFlow agent periodically collects traffic statistics on an interface, CPU usage, and memory usage. sFlow focuses on traffic on an interface, traffic forwarding, and device operation, so it can be used to monitor and locate network exceptions. The sFlow collector displays the traffic statistics in a report, which facilitates preventive maintenance especially on enterprise networks without specialized network administrators.

Copyright © Huawei Technologies Co., Ltd.

NetStream is a technology that collects and analyzes statistics on network flows. Network devices need to preliminarily collect and analyze network flows, and store statistics in the cache. When the cache overflows or flow statistics expire, the statistics are exported. Compared with NetStream, sFlow does not require a cache, network devices only sample packets, and a remote collector collects and analyzes traffic statistics. Therefore, sFlow has the following advantages over NetStream:

- Saves resources and lowers costs. No cache is required, and a small number of network devices are used, which lower costs.
- Flexible collector deployment. A collector collects and analyzes traffic statistics based on various traffic characteristics as required. The collector is deployed flexibly.

1.2 References

The following table lists the references of this document.

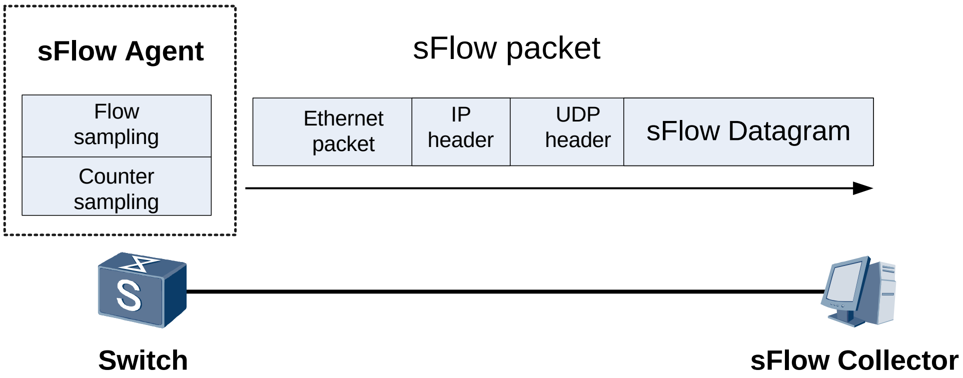
Document	Description	Remarks
sFlow version 5	Inmon sFlow version 5	-
RFC 3176	Inmon sFlow version 4	-
RFC 1014	XDR: External Data Representation Standard	-

1.3 Principles

1.3.1 Architecture of an sFlow System

As shown in Figure 1-1, the sFlow system involves an sFlow agent embedded in the device and a remote sFlow collector. The sFlow agent obtains traffic statistics from an sFlow-enabled interface using sFlow sampling and encapsulates them into sFlow packets. When an sFlow packet buffer overflows or an sFlow packet expires, the sFlow agent sends the sFlow packets to the sFlow collector. The sFlow collector analyzes the sFlow packets and displays the traffic statistics in a report.

Figure 1-1 sFlow system



NOTE

- A switch often serves as an sFlow agent. Therefore, this section describes the sFlow agent implementation and configuration.

An sFlow collector is a PC or server. It is responsible for receiving sFlow packets sent from an sFlow agent, without having special requirements for the hardware and operating system. The client software needs to be installed on an sFlow collector to analyze sFlow packets. The sFlow Trend is a free software client that analyzes sFlow packets. You can visit the website www.sflow.org to install the sFlow Trend or download the software usage guide.

1.3.2 sFlow Packet Format

Figure 1-1 shows the sFlow packet format. sFlow packets are encapsulated in UDP packets. By default, sFlow packets are transmitted by known port 6343. sFlow packets use the following packet header formats: Flow sample, Expanded Flow sample, Counter sample, and Expanded Counter sample. Expanded Flow sample and Expanded Counter sample are added to sFlow version5 and are extensions to Flow sample and Counter sample, but they are not compatible with earlier versions. All expanded sampling packets must be encapsulated with the expanded sampling packet header.

1.3.3 sFlow Sampling

An sFlow agent provides two sampling modes: flow sampling and counter sampling.

Flow sampling

In flow sampling, an sFlow agent samples packets in one direction or both directions on an interface based on the sampling ratio, and parses the packets to obtain information about packet data content. Table 1-1 lists the main fields in flow sampling packets. Flow sampling focuses on traffic details to monitor and parse traffic behaviors on the network.

Flow sampling samples packets on an interface, and currently supports only random sampling. In random sampling mode, the sFlow agent allocates a random value to each packet processed by an interface. The random value ranges from 0 to N. The threshold is set to n ranging from 0 to N. When the random value is smaller than the threshold, the sFlow agent samples packets. The actual sampling ratio is n/(N+1).

Table 1-1 Main fields in flow sampling packets

Field	Description
Raw packet	Records the entire packet or part of the packet header, encapsulates the recorded raw packets to an sFlow packet, and sends the sFlow packet to the collector.
Ethernet Frame Data	Analyzes Ethernet headers in Ethernet frames, encapsulates the analyzed Ethernet header to an sFlow packet, and sends the sFlow packet to the collector.
IPv4 Data	Records IPv4 header information in IPv4 packets.
IPv6 Data	Records IPv6 header information in IPv6 packets.
Extended	Records VLAN translation and 802.1Q priority mapping

Field	Description
Switch Data	information in Ethernet frames. VLAN 0 is an invalid VLAN.
Extended Router Data	Records routing information for packets.

Counter sampling

An sFlow agent periodically obtains traffic statistics on an interface. Table 1-2 lists the main fields in counter sampling packets. Compared with flow sampling, counter sampling focuses on traffic statistics on an interface rather than traffic details.

Table 1-2 Main fields in counter sampling packets

Field	Description
Generic Interface Counters	Records basic information and traffic statistics on an interface.
Ethernet Interface Counters	Records traffic statistics on an Ethernet interface.
Processor Information	Records CPU usage and memory usage of a device.

Flow sampling and counter sampling are independent of each other. Flow sampling obtains information about flows of a specified service, whereas counter sampling obtains traffic statistics on an interface. It is recommended that you use both the two sampling modes.

1.4 Applications

1.4.1 Network Monitoring

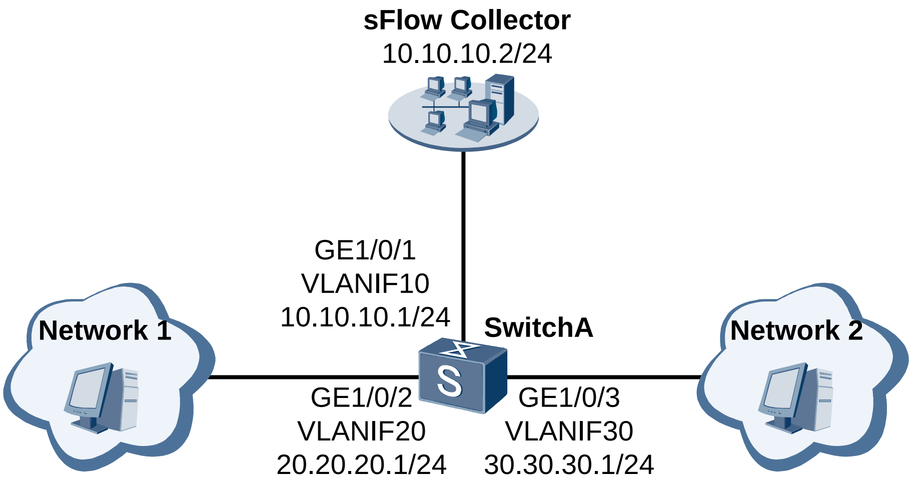
Network maintenance personnel often use the traffic monitoring technique to monitor networks.

Enterprise network users often have requirements for traffic on an interface and device running. They require a traffic monitoring technique on an interface to locate unexpected traffic and the source of attack traffic immediately so that they can rectify faults quickly to ensure stable running of the network.

As shown in Figure 1-2, traffic is exchanged between Network1 and Network2 through SwitchA. The maintenance personnel need to monitor the traffic on interfaces and device operation to locate unexpected traffic and ensure normal network operation. Before collecting traffic statistics on an interface and analyzing the collected traffic statistics, configure SwitchA as an sFlow agent and connect the sFlow agent to an sFlow collector.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-2 sFlow agent configuration



Configuration roadmap:

Run the sFlow agent on SwitchA. Enable sFlow sampling functions on GE1/0/2 including flow sampling and counter sampling.
After the previous configurations are complete, the sFlow agent sends sFlow packets containing traffic statistics from GE1/0/1 to the sFlow collector. The sFlow collector displays network traffic according to the received sFlow packets. In this way, traffic on GE1/0/2 is monitored.

# Configuration file of SwitchA

```
#
sysname SwitchA
#
vlan batch 10 20 30
#
interface Vlanif10
 ip address 10.10.10.1 255.255.255.0
#
interface Vlanif20
 ip address 20.20.20.1 255.255.255.0
#
interface Vlanif30
 ip address 30.30.30.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 10
#
interface GigabitEthernet1/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
 sflow counter-sampling collector 1
 sflow flow-sampling collector 1
#
interface GigabitEthernet1/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
sflow collector 1 ip 10.10.10.2 description netserver
#
sflow agent ip 10.10.10.1
#
return
```

1.5 Troubleshooting

1.5.1 A Remote sFlow Collector Fails to Receive sFlow Packets

Fault Symptom

A remote sFlow collector fails to receive sFlow packets.

Procedure

Step 1 Check whether an IP address is configured for the sFlow collector.

Run the **display sflow** command to view the configuration. If the **Collector Information** is null, run the **sflow collector** command in the system view to configure the IP address and other related attributes for the sFlow collector.

```
<Quidway> display sflow slot 1
sFlow Version 5 Information:
--------------------------------------------------------------------------
Agent Information:
  IP Address: 192.168.1.206
  Address family: IPV4
  Vpn-instance: N/A
--------------------------------------------------------------------------
Collector Information:
  Collector ID: 1
  IP Address: 192.168.1.194
  Address family: IPV4
  Vpn-instance: N/A
  Port: 6343
  Datagram size: 1500
  Time out: N/A
  Description: zjm-pc
--------------------------------------------------------------------------
Port on slot 1 Information:
Interface: GE1/0/1
  Flow-sample collector: 1          Counter-sample collector  : 1
  Flow-sample rate(1/x): 2048       Counter-sample interval(s): 10
  Flow-sample maxheader: 128
  Flow-sample direction: IN,OUT
```

Step 2 Check whether the configured IP address of the sFlow collector is the same as the IP address of the remote sFlow collector.

If the IP addresses are different, the remote sFlow collector cannot receive sFlow packets.

Run the **display sflow** command to view the configuration. If the IP address in the **Collector Information** is different from the IP address of the remote sFlow collector, run the **sflow collector** command in the system view to configure a correct IP address for the sFlow collector.

```
<Quidway> display sflow slot 1
sFlow Version 5 Information:
--------------------------------------------------------------------------
Agent Information:
  IP Address: 192.168.1.206
  Address family: IPV4
  Vpn-instance: N/A
--------------------------------------------------------------------------
Collector Information:
  Collector ID: 1
  IP Address: 192.168.1.194
  Address family: IPV4
  Vpn-instance: N/A
  Port: 6343
  Datagram size: 1500
  Time out: N/A
  Description: zjm-pc
--------------------------------------------------------------------------
Port on slot 1 Information:
Interface: GE1/0/1
  Flow-sample collector: 1          Counter-sample collector  : 1
  Flow-sample rate(1/x): 2048       Counter-sample interval(s): 10
  Flow-sample maxheader: 128
  Flow-sample direction: IN,OUT
```

Step 3 Check whether sFlow sampling is configured on the interface.

If sFlow sampling is not configured on the interface, the interface does not provide sampling data.

Run the **display sflow** command to view the configuration. If the **Port on slot 1 Information** is null, select flow sampling or counter sampling. It is recommended that you configure both flow sampling and counter sampling.

```
<Quidway> display sflow slot 1
sFlow Version 5 Information:
--------------------------------------------------------------------------
Agent Information:
  IP Address: 192.168.1.206
  Address family: IPV4
  Vpn-instance: N/A
--------------------------------------------------------------------------
Collector Information:
  Collector ID: 1
  IP Address: 192.168.1.194
  Address family: IPV4
  Vpn-instance: N/A
  Port: 6343
  Datagram size: 1500
  Time out: N/A
  Description: zjm-pc
```

```
--------------------------------------------------------------------------
Port on slot 1 Information:
Interface: GE1/0/1
  Flow-sample collector: 1          Counter-sample collector  : 1
  Flow-sample rate(1/x): 2048       Counter-sample interval(s): 10
  Flow-sample maxheader: 128
  Flow-sample direction: IN,OUT
```

----End

1.6 Terms and Abbreviations

Terms

Term	Description
sFlow Agent	Device embedded in a network device. An sFlow agent collects traffic statistics and sends the traffic statistics to an sFlow collector.
sFlow Collector	Device that receives sFlow packets from sFlow agents and displays traffic in icons or reports.

Abbreviations

Acronyms	Full Spelling
sFlow	Sampled flow