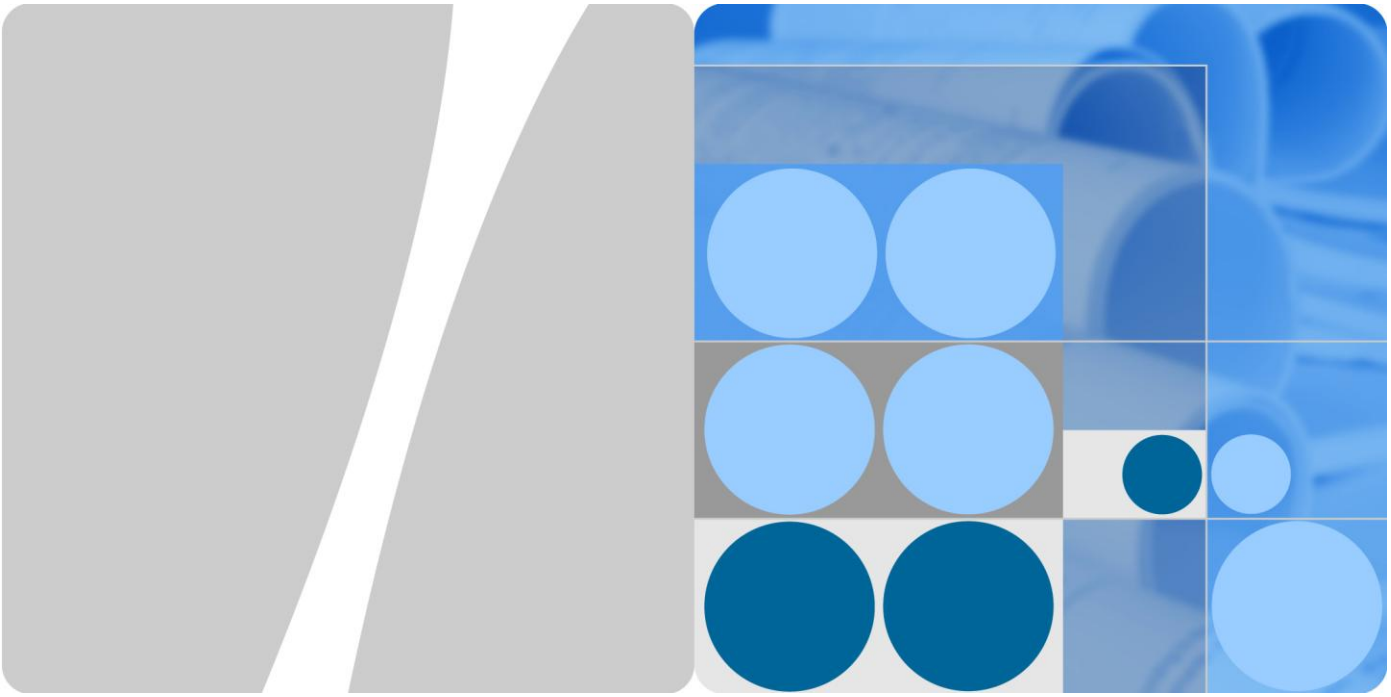


# sFlow 技术白皮书

文档版本 01

发布日期 2012-10-30

华为技术有限公司

**商标声明**


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

**注意**

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。


# 华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

# 1 sFlow

## 关于本章



## 1.1 介绍

### 定义

采样流 sFlow（Sampled Flow）是一种基于报文采样的网络流量监控技术，主要用于对网络流量进行统计分析。

### 目的

相对于电信级网络，企业级网络通常具有规模相对较小、组网灵活、易受攻击等特点，因此企业级网络更容易出现由组网或者攻击导致的流量业务异常。于是企业用户更需要一种以设备接口为基本采样单元的流量监控技术来实时监控流量状况，及时发现异常流量以及攻击流量的源头，从而保证企业网络的正常稳定运行。

这样的背景下，sFlow 应运而生。sFlow 是基于端口的流量分析：按照一定的采样比从特定端口上采集报文，由 Agent 设备对报文进行分析（包括报文内容、报文转发规则信息等等），并将分析结果以及原始报文通告给 Collector 进行统一分析（Flow 采样）；并且支持周期性统计端口的流量计数以及设备 CPU、内存等信息（Counter 采样）。sFlow 关注的是接口的流量情况、转发情况以及设备整体运行状况，因此适合于网络异常监控以及网络异常定位，通过 Collector 可以以报表的方式将情况反应出来，特别适

合于企业网用户。为企业用户（特别是未设置专职网络管理员的企业用户）的日常巡检维护提供了极大的方便。

使用 NetStream 也可以对网络流量进行统计分析，而 NetStream 是一种基于网络流信息的统计技术，网络设备自身需要对网络流进行初步的统计分析，并把统计信息储存在缓存区，当缓存区满或者流统计信息老化后输出统计信息。与 NetStream 相比，sFlow 不需要缓存区，网络设备仅进行报文的采样工作，网络流的统计分析工作由远端的采集器完成。因此 sFlow 与 NetStream 比较具有以下优势：

- 节省资源、降低成本：由于不需要缓存区，对网络设备的资源占用少，实现成本低。
- 采集器灵活、随需的部署：由于网络流的分析和统计工作由采集器完成，采集器可以灵活的配置网络流特征进行统计分析，实现灵活、随需的部署。

# 1.2 参考标准和协议

本特性的参考资料清单如下：

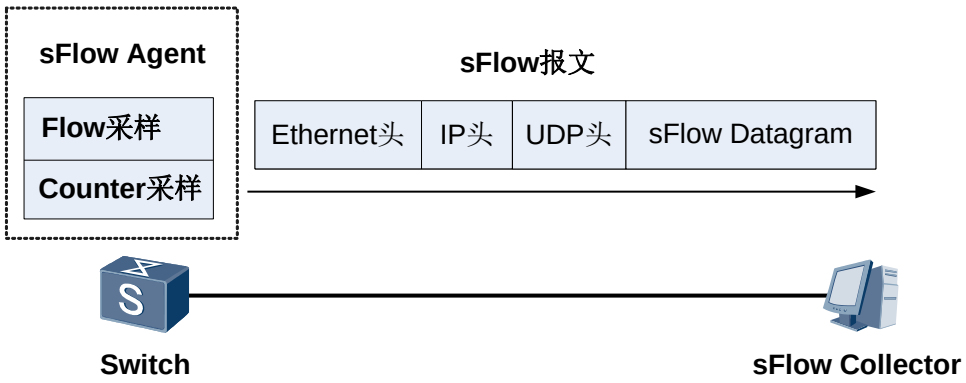
| 文档 | 描述 | 备注 |
| --- | --- | --- |
| sFlow version 5 | Inmon sFlow version 5 | - |
| RFC 3176 | Inmon sFlow version 4 | - |
| RFC 1014 | XDR: External Data Representation Standard | - |

# 1.3 原理描述

## sFlow 系统组成

如图 1-1 所示，sFlow 系统包含一个嵌入在设备中的 sFlow Agent 和远端的 sFlow Collector。其中，sFlow Agent 通过 **sFlow 采样**获取本设备上的接口统计信息和数据信息，将信息封装成 **sFlow 报文**，当 sFlow 报文缓冲区满或是在 sFlow 报文缓存时间（缓存时间为 1 秒）超时后，sFlow Agent 会将 sFlow 报文发送到指定的 sFlow Collector。sFlow Collector 对 sFlow 报文进行分析，并显示分析结果。

图1-1 sFlow 系统示意图




说明

- 由于设备在 sFlow 功能中担任 sFlow Agent 的角色，所以本文档重点介绍 sFlow Agent 的实现以及配置。
- sFlow Collector 可以是 PC 或者服务器，负责接收 sFlow Agent 发送的 sFlow 报文，对硬件和操作系统没有特殊要求。在 sFlow Collector 上需要安装针对 sFlow 报文进行分析的客户端软件。sFlow Trend 是一款免费的针对 sFlow 报文流量分析的客服端软件，可以登录 sflow.org 网站进行在线安装以及下载软件使用指南。

## sFlow 报文

sFlow 的报文格式如图 1-1 中 sFlow 报文所示，采用 UDP 封装，缺省目的端口号为知名端口 6343。sFlow 报文共有 4 种报文头格式，分别为 Flow sample、Expanded Flow sample、Counter sample、Expanded Counter sample。其中 Expanded Flow sample 和 Expanded Counter sample 是 sFlow version 5 新增内容，是 Flow sample 和 Counter sample 的扩展，但不前向兼容。所有的 Extended 的采样内容必须使用 Expanded 采样报文头封装。

## sFlow 采样

sFlow Agent 提供了两种采样方式供用户从不同的角度分析网络流量状况，分别为 Flow 采样以及 Counter 采样。

**Flow 采样**

Flow 采样是 sFlow Agent 设备在指定端口上按照特定的采样方向和采样比对报文进行采样分析，用于获取报文数据内容的相关信息，Flow 采样支持获取的采样信息如表 1-1 所示。该采样方式主要是关注流量的细节，这样就可以监控和分析网络上的流行为。

Flow 采样是针对接口上报文的采样方式，目前仅支持报文随机采样模式。随机采样模式是指针对每一个接口处理的报文给一个随机值（假定随机数的取值范围为 0～N），设置一个阈值 n（n 属于 0～N，范围包含 0 和 N），当报文的随机值小于这个阈值时，报文采样，这样实际的采样比为 n/(N+1)。

表1-1 Flow 采样报文中主要字段信息说明

| 字段内容 | 说明 |
| --- | --- |
| Raw packet | 截取原始报文全部或者一部分报文头（具体截取多长的长度由配置决定），将这部分原始报文封装到 sFlow 报文中发送给 Collector。 |
| Ethernet Frame Data | 针对 Ethernet 报文，解析报文的 Ethernet 头信息，将解析数据封装到 sFlow 报文中发送给 Collector。 |
| IPv4 Data | 针对 IPv4 报文，解析报文的 IPv4 头信息，将解析数据封装到 sFlow 报文中发送给 Collector。 |
| IPv6 Data | 针对 IPv6 报文，解析报文的 IPv6 头信息，将解析数据封装到 sFlow 报文中发送给 Collector。 |
| Extended Switch Data | 针对二层转发的 Ethernet 报文，记录报文的 VLAN 转换以及 VLAN 优先级的转换，将转发信息封装到 sFlow 报文中发送给 Collector。VLAN ID 为 0 时表示无效 VLAN。 |
| Extended Router Data | 针对路由转发的报文，记录报文的路由转发信息，将转发信息封装到 sFlow 报文中发送给 Collector。 |

**Counter 采样**

Counter 采样是 sFlow Agent 设备周期性的获取接口上的流量统计信息，Counter 采样支持获取的采样信息如表 1-2 所示。与 Flow 采样相比，Counter 采样只关注接口上流量的量，而不关注流量的详细信息。

表1-2 Counter 采样报文中主要字段信息说明

| 字段内容 | 说明 |
| --- | --- |
| Generic Interface Counters | 通用接口统计信息，包括接口的基本信息，通用的接口流量统计。 |
| Ethernet Interface Counters | 针对于 Ethernet 接口，用于统计 Ethernet 相关的流量统计信息。 |
| Processor Information | 用于统计设备 CPU 占用率，内存使用情况。 |

Flow 采样和 Counter 采样是两种相互独立的采样，两者互相没有影响。但是由于采样的方式不一样，获取的信息维度也不一样，Flow 方式更聚焦于具体的流的分析，可以搜集具体业务的相关数据。而 Counter 方式更聚焦于接口的统计信息，对于整体的网络状态监控比较有意义。在应用时可以根据需要进行配置，一般情况下建议都配置。

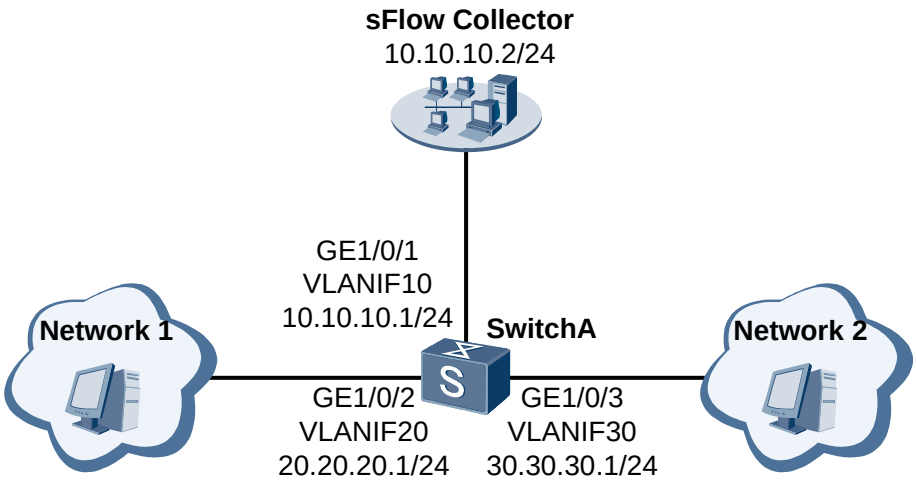
# 1.4 应用

## 网络监管

网络监管是网络维护人员常见的场景，其中流量监管是网络监管的一个基础技术。

如图 1-2 所示，企业两个网络 Network1 与 Network2 之间通过 SwitchA 互发流量。网络维护人员需要监控接口的流量信息、转发情况以及设备的整体运行状况，及时发现异常流量，从而保证网络的正常稳定运行。此时，只需要在 SwitchA 设备上部署 sFow Agent 功能，远端连接一个 sFlow Collector，就可以对流量进行基于端口的搜集和详细的分析。

图1-2 配置 sFlow 功能组网图




配置思路：

在 SwitchA 上运行 sFlow Agent，通过在 GE1/0/2 上开启 sFlow 采样功能（包括 Flow 采样和 Counter 采样），sFlow Agent 能够将采集到的流量统计信息通过 sFlow 报文从 GE1/0/1 发向 sFlow Collector，然后 sFlow Collector 根据收到的 sFlow 报文中携带的流量信息，将网络流量状况显示出来。从而实现对 GE1/0/2 接口流量信息的监控。

# SwitchA 的配置文件：

```
#
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 故障处理

## 1.5.1 远端的 sFlow Collector 无法收到 sFlow 报文

### 故障现象

远端的 sFlow Collector 无法收到 sFlow 报文。

### 操作步骤

步骤 1 检查是否配置 sFlow Collector 的 IP 地址

执行 **display sflow** 命令查看配置信息，如果 **Collector Information** 为空，请在系统视图下执行 **sflow collector** 命令配置 sFlow Collector 的 IP 地址以及其它相关属性。

```
<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
```

步骤 2 检查配置的 sFlow Collector 的 IP 地址和远端的 sFlow Collector 的 IP 地址是否相同

如果 IP 地址不相同，导致远端的 sFlow Collector 无法收到 sFlow 报文。

执行 **display sflow** 命令查看配置信息，如果 **Collector Information** 中的 IP 地址信息与远端的 sFlow Collector 的 IP 地址不相同，请在系统视图下执行 **sflow collector** 命令配置 sFlow Collector 的正确 IP 地址。

```
<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
```

步骤 3 检查接口是否配置 sFlow 采样

接口如果没有配置 sFlow 采样，导致没有接口提供采样数据。

执行 **display sflow** 命令查看配置信息，如果 **Port on slot 1 Information** 为空，请选择配置 sFlow 采样中 Flow 采样或者 Counter 采样进行配置，一般建议同时配置 Flow 采样和 Counter 采样。

```
<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
```

# 1.6 术语与缩略语

## 术语

| 术语 | 解释 |
| --- | --- |
| sFlow Agent | 内嵌于网络设备中，在 sFlow 系统中收集流量统计数据发送到 Collector 端供分析。 |
| sFlow Collector | 通常由专门服务器充当，在 sFlow 系统中收集各 Agent 的采样数据并以图标或报表的形式加以汇总。 |

## 缩略语

| 缩略语 | 英文全称 | 中文全称 |
| --- | --- | --- |
| sFlow | Sampled flow | 流采样 |