

目录

第 1 章 镜像	1-1
1.1 镜像介绍	1-1
1.2 镜像配置任务序列	1-1
1.3 镜像举例	1-2
1.4 镜像排错帮助	1-2
第 2 章 RSPAN 配置	2-1
2.1 RSPAN 简介	2-1
2.2 RSPAN 配置任务序列	2-2
2.3 RSPAN 典型案例	2-3
2.4 RSPAN 排错帮助	2-6
第 3 章 sFlow 配置	3-1
3.1 sFlow 介绍	3-1
3.2 sFlow 配置任务序列	3-1
3.3 sFlow 举例	3-3
3.4 sFlow 排错帮助	3-3
第 4 章 IPFIX 配置	4-1
4.1 IPFIX 介绍	4-1
4.2 IPFIX 基本配置	4-1
4.3 IPFIX 举例	4-5
4.4 IPFIX 排错帮助	4-7
第 5 章 ERSPAN 配置	5-1
5.1 ERSPAN 简介	5-1
5.2 ERSPAN 配置任务序列	5-1
5.3 ERSPAN 典型案例	5-1
5.4 ERSPAN 排错帮助	5-3

第1章 镜像

1.1 镜像介绍

镜像功能包括端口镜像功能，CPU 镜像功能，流镜像功能。

端口镜像功能是指交换机把某一个端口接收或发送的数据帧完全相同的复制给另一个端口；其中被复制的端口称为镜像源端口，复制的端口称为镜像目的端口。通常在镜像目的端口处连接一个协议分析仪（如 Sniffer）或者 RMON 监测仪，可以监视和管理网络，并且能诊断网络故障。

CPU 镜像功能是指交换机把 CPU 接收或发送的数据帧完全复制给一个端口。

流镜像功能是指交换机把端口的指定规则的接收的数据帧完全复制给一个端口，其中指定规则只有为 permit 时流镜像才能生效。

该机架式交换机支持最多 36 个镜像目的端口，每个板卡上允许设置 4 个镜像 session 的源或者目的端口，对于盒式交换机目前能设置多个镜像 session。镜像源端口则没有使用上的限制，可以是 1 个也可以是多个，多个源端口可以在相同的 VLAN，也可以在不同 VLAN。目的端口和源端口可以在不同的 VLAN。

1.2 镜像配置任务序列

1. 指定镜像目的端口
2. 指定镜像源端口（CPU）
3. 指定流镜像源

1. 指定镜像目的端口

命令	解释
全局配置模式	
monitor session <session> destination interface <interface-number> no monitor session <session> destination interface <interface-number>	指定镜像目的端口；本命令的 no 操作为删除镜像目的端口。

2. 指定镜像源端口（CPU）

命令	解释
全局配置模式	
monitor session <session> source {interface <interface-list> cpu {slot <slotnum> member <memberid> slot <slotnum> }} {rx tx both} no monitor session <session> source {interface <interface-list> cpu [slot <slotnum>]}	指定镜像源端口；本命令的 no 操作为删除镜像源端口。

3. 指定流镜像源

命令	解释
全局配置模式	
monitor session <session> source {interface <interface-list>} access-group <num> {rx tx both} no monitor session <session> source {interface <interface-list>} access-group <num>	指定流镜像源端口及应用规则；本命令的 no 操作为删除流镜像源端口。

1.3 镜像举例

案例：

用户有如下的配置需求：为了在 1 端口监测 7 端口接收的数据帧和 9 端口发出的数据帧，同时还要监测 CPU 接收和发出的数据帧，端口 15 的符合规则 120（源 IP 为 1.2.3.4,目的 IP 为 5.6.7.8）的入口的数据帧，通过配置镜像来达到这个目的。

配置修改：

- 1: 配置 1 端口为该镜像的镜像目的；
- 2: 配置 7 端口的入口方向和 9 端口的出口方向为镜像源；
- 3: 配置 cpu 为镜像源；
- 4: 配置规则 120；
- 5: 配置端口 15 的入口绑定规则 120。

配置步骤如下：

```
Switch(config)#monitor session 4 destination interface ethernet 1/1
Switch(config)#monitor session 4 source interface ethernet 1/7 rx
Switch(config)#monitor session 4 source interface ethernet 1/9 tx
Switch(config)#monitor session 4 source cpu
Switch(config)#access-list 120 permit tcp 1.2.3.4 0.0.0.255 5.6.7.8 0.0.0.255
Switch(config)#monitor session 4 source interface ethernet 1/15 access-list 120 rx
```

1.4 镜像排错帮助

当配置镜像功能出现问题时，请检查是否是如下原因：

- ✧ 镜像目的端口是端口聚合组成员；如果是，请修改端口聚合组。
- ✧ 镜像目的端口的吞吐量小于镜像源端口吞吐量的总和，目的端口无法完全复制源端口的流量；请减少源端口的个数或复制单向的流量，或者选择吞吐量更大的端口作为目的端口。镜像目的端口不能划入 Isolate vlan，否则将影响跨 VLAN 镜像。

第2章 RSPAN 配置

2.1 RSPAN 简介

端口镜像功能是指交换机把某一个端口接收或发送的数据帧完全相同的复制给另一个端口。其中被复制的端口称为镜像源端口，复制到的端口称为镜像目的端口。镜像功能的出现，给网管人员诊断网络故障带了很多的方便。但美中不足的是，它只局限于镜像源端口和镜像目的端口处于同一交换机的情况。

RSPAN (remote switched port analyzer, 远程交换端口分析)，即远程端口镜像，突破了镜像源和目的端口必须处于同一交换机的限制，使镜像源端口和镜像目的端口可以在不同的网络设备上，从而方便网管人员对远程交换机设备进行管理。在远程镜像的 vlan 上不能进行业务流的传输。

实现了 RSPAN 功能的交换机分为三种：

1. 源交换机：被监测的端口所在的交换机，负责将需要镜像的流量在 Remote VLAN 上做二层转发，转发给中间交换机或目的交换机。
2. 中间交换机：网络中处于源交换机和目的交换机之间的交换机，把镜像流量传输给下一个中间交换机或目的交换机。如果源交换机与目的交换机直接相连，则不存在中间交换机。
3. 目的交换机：远程镜像目的端口所在的交换机，将从 Remote VLAN 接收到的镜像流量通过镜像目的端口转发给监控设备。

在配置源交换机的 rspan 镜像时可以采用反射端口或直接镜像到目的端口的方式。在目的交换机端将 RSPAN vlan 上的数据发送到 RSPAN 目的端口。我们采用一般模式和高级模式两种，其中一般作为默认方法，适合一般用户。高级模式，适合高级用户。

- 1.高级模式特性：RSPAN vlan 的数据重定向到 RSPAN 目的端口需要 RSPAN 链路的中间和目的设备支持流的重定向的功能。
- 2.一般模式特性：RSPAN 目的端口划入 RSPAN vlan，这样 RSPAN 的数据直接广播到目的端口。目的端口局限于 RSPAN vlan，源端口不能配置广播抑制。需要小心配置各个 Trunk 端口，防止 RSPAN 数据向其他网络转发。由于采用一般方式，占用资源最少、配置简单。

注：默认采用一般模式。采用一般模式时，如果镜像的报文的 MAC 地址是保留地址则无法广播

该机架式交换机支持最多 36 个镜像目的端口，每个板卡上允许设置 4 个镜像 session 的源或者目的端口，对于盒式交换机目前只能设置一个镜像 session。镜像源端口则没有使用上的限制，可以是 1 个也可以是多个，多个源端口可以在相同的 VLAN，也可以在不同 VLAN。目的端口和源端口可以在不同的 VLAN。

在使用 RSPAN 功能之前，要先创建专属的 RSPAN vlan，用于转发 RSPAN 数据报文不能在这个 vlan 上承载业务。由于默认情况下所有的端口都属于缺省 vlan，在标记 RSPAN vlan 时禁止将缺省 vlan、动态 vlan、私有 vlan、组播 vlan、配置了三层接口的 vlan 等特殊 vlan 配置为 RSPAN vlan。目的端口与 Monitor 相连，该端口必须为 access 端口且属于 RSPAN vlan。反射端口必须属于 RSPAN vlan，可以为 RSPAN vlan 的 access 口，或者为 trunk 口。端口被配置为 RSPAN 的反射端口之后自动失去与对端的连接并禁止在反射端口上做 loopback 相关的配置，同时其他的业务数据也将无法转发，所以反射端口要求必须是

专用的端口。需要通过配置保证 Remote VLAN 从源交换机到目的交换机的二层互通性。

需要注意的问题：

- 1.在源交换机、中间交换机和目的交换机的 RSPAN vlan 上都不能起三层接口，否则镜像后的报文有可能被丢弃而无法到达目的端口。
- 2.在源交换机和中间交换机的 RSPAN 数据传输链路中，交换机输出方向的 Trunk 端口的 native vlan 不能设置为 RSPAN vlan，否则 RSPAN tag 在没有到达目的交换机时就会被剥离掉，从而导致 RSPAN 失败。
- 3.在源交换机采用反射端口的镜像方式时，不能把镜像的源端口以 access 或者是 trunk 的方式配置为 RSPAN VLAN 的成员端口。采用反射端口做跨板的 cpu tx 方向镜像时，反射端口必须配置为 trunk 端口允许 RSPAN VLAN 的数据通过，并且其 native vlan 不能配置为 RSPAN VLAN。
- 4.在使用远程镜像时需注意链路的带宽要满足业务流和镜像流量的需要。
- 5.采用反射端口的方式作 RSPAN 的情况下，为防止镜像源的业务流量在某种情况下环回到镜像目的端口，造成镜像目的端口学习到业务流量的 src mac，从而导致 rspan vlan 的流量由广播变为单播流量转发到镜像目的端口，建议关闭镜像目的端口的源 mac 学习。

名词解释：

- RSPAN(remote switched port analyzer)：远程交换端口分析。
- RSPAN vlan：专用于 RSPAN 的一个特殊 vlan。
- RSPAN Tag：RSPAN 数据在 MTP 上被打上的一个 Vlan Tag
- 反射端口：从 RSPAN 源端口到本地目的端口的本地镜像。但这个本地目的端口不直接与中间交换机相连，我们把这个端口叫做反射端口。

2.2 RSPAN 配置任务序列

- 1. 配置 rspan vlan
- 2. 指定镜像源端口（cpu）
- 3. 指定镜像目的端口
- 4. 配置反射端口
- 5. 配置镜像组的 remote vlan

1. 配置 RSPAN vlan

命令	解释
Vlan 配置模式	
remote-span no remote-span	将当前 vlan 配置为 rspan vlan；no 操作为删除 rspan vlan。

2. 指定镜像源端口(CPU)

命令	解释
全局配置模式	

monitor session <session> source {interface <interface-list> cpu [slot <slotnum>]} {rx tx both} no monitor session <session> source {interface <interface-list> cpu [slot <slotnum>]}	指定镜像源端口；本命令的 no 操作为删除镜像源端口。
--	-----------------------------

3. 指定镜像目的端口

命令	解释
全局配置模式	
monitor session <session> destination interface <interface-number> no monitor session <session> destination interface <interface-number>	指定镜像目的端口；本命令的 no 操作为删除镜像目的端口。

4. 配置反射端口

命令	解释
全局配置模式	
monitor session <session> reflector-port <interface-number> no monitor session <session> reflector-port	将端口配置为反射端口，使用 no 命令删除反射端口。

5. 配置镜像组的 remote vlan

命令	解释
全局配置模式	
monitor session <session> remote vlan <vid> no monitor session <session> remote vlan	配置镜像组的 remote valn，no 操作为删除镜像组的 remote vlan。

2.3 RSPAN 典型案例

在没有 RSPAN 之前，网络管理人员需要带着笔记本电脑跑到各个交换机处，将电脑连接到交换机上，才能检测网络的状况，非常不方便。

而有了 RSPAN 功能之后，管理员只需要在网管中心通过 Telnet 做一些简单的配置，就能检测到任何一台交换机（当然，这台交换机需要支持 RSPAN 功能）的运行状况。大大方便了网管人员的管理工作。下图是 RSPAN 功能的一种应用：

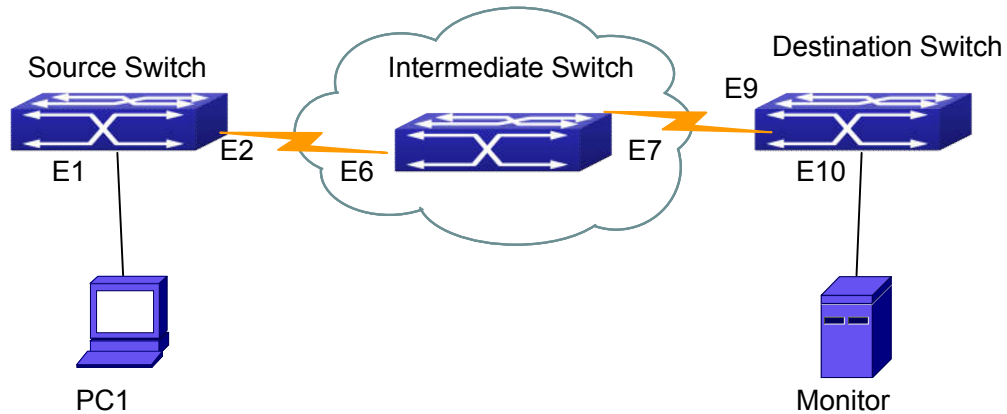


图 2-1 RSPAN 应用示意图

可以采用两种方案：方案一无反射端口，方案二有反射端口：方案一只能固定一个端口与中间交换机连接，方案二源与中间交换机连接端口不固定，比较灵活；

两种方案的比较：方案一虽说只能固定一个接口与中间交换机连接，但是它省去了一个反射端口，端口利用率高。方案二通过反射端口，可以将数据报文通过回环在 RSPAN vlan 中广播，灵活的与中间交换机通信。

以下是采用一般模式转发时各个交换机的配置：

方案一：

源交换机：

interface ethernet 1/1 为源端口。

interface ethernet 1/2 为目的端口，与中间交换机相连。

RSPAN vlan 为 5。

```
Switch(config)#vlan 5
Switch(Config-Vlan5)#remote-span
Switch(Config-Vlan5)#exit
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#switchport mode trunk
Switch(Config-If-Ethernet1/2)#exit
Switch(config)#monitor session 1 source interface ethernet1/1 rx
Switch(config)#monitor session 1 destination interface ethernet1/2
Switch(config)#monitor session 1 remote vlan 5
```

中间交换机：

interface ethernet1/6 为源端口，与源交换机相连。

interface ethernet1/7 为目的端口，与目的交换机相连，该端口的 native vlan 不能设置为 RSPAN vlan，否则镜像后的数据可能无法在目的交换机上正确传输。

RSPAN vlan 为 5。

```
Switch(config)#vlan 5
Switch(Config-Vlan5)#remote-span
Switch(Config-Vlan5)#exit
Switch(config)#interface ethernet 1/6-7
```

```
Switch(Config-If-Port-Range)#switchport mode trunk
Switch(Config-If-Port-Range)#exit
```

目的交换机:

interface ethernet1/9 为源端口, 与源交换机相连。

interface ethernet1/10 为目的端口, 与 Monitor 相连, 该端口必须为 access 端口且属于 RSPAN vlan。

RSPAN vlan 为 5。

```
Switch(config)#vlan 5
Switch(Config-Vlan5)#remote-span
Switch(Config-Vlan5)#exit
Switch(config)#interface ethernet 1/9
Switch(Config-If-Ethernet1/9)#switchport mode trunk
Switch(Config-If-Ethernet1/9)#exit
Switch(config)#interface ethernet 1/10
Switch(Config-If-Ethernet1/10)#switchport access vlan 5
Switch(Config-If-Ethernet1/10)#exit
```

方案二:

源交换机:

interface ethernet 1/1 为源端口。

interface ethernet 1/2 为 trunk 端口, 与中间交换机相连, 该端口的 native vlan 不能为 RSPAN vlan。

interface ethernet 1/3 为反射端口, 也是本地镜像目的端口, 反射端口必须属于 RSPAN vlan, 可以为 RSPAN vlan 的 access 口, 或者为 trunk 口。

RSPAN vlan 为 5。

```
Switch(config)#vlan 5
Switch(Config-Vlan5)#remote-span
Switch(Config-Vlan5)#exit
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#switchport mode trunk
Switch(Config-If-Ethernet1/2)#exit
Switch(config)#interface ethernet 1/3
Switch(Config-If-Ethernet1/3)#switchport mode trunk
Switch(Config-If-Ethernet1/3)#exit
Switch(config)#monitor session 1 source interface ethernet1/1 rx
Switch(config)#monitor session 1 reflector-port ethernet1/3
Switch(config)#monitor session 1 remote vlan 5
```

中间交换机:

interface ethernet1/6 为源端口, 与源交换机相连。

interface ethernet1/7 为目的端口, 与目的交换机相连, 该端口的 native vlan 不能设置为

RSPAN vlan，否则镜像后的数据可能无法在目的交换机上正确传输。

RSPAN vlan 为 5。

```
Switch(config)#vlan 5
Switch(Config-Vlan5)#remote-span
Switch(Config-Vlan5)#exit
Switch(config)#interface ethernet 1/6-7
Switch(Config-If-Port-Range)#switchport mode trunk
Switch(Config-If-Port-Range)#exit
```

目的交换机：

interface ethernet1/9 为源端口，与源交换机相连。

interface ethernet1/10 为目的端口，与 Monitor 相连，该端口必须为 access 端口且属于 RSPAN vlan。

RSPAN vlan 为 5。

```
Switch(config)#vlan 5
Switch(Config-Vlan5)#remote-span
Switch(Config-Vlan5)#exit
Switch(config)#interface ethernet 1/9
Switch(Config-If-Ethernet1/9)#switchport mode trunk
Switch(Config-If-Ethernet1/9)#exit
Switch(config)#interface ethernet 1/10
Switch(Config-If-Ethernet1/10)#switchport access vlan 5
Switch(Config-If-Ethernet1/10)#exit
```

2.4 RSPAN 排错帮助

当配置 rspan 功能出现问题时，请检查是否是如下原因：

- ☞ 镜像目的端口是否是端口聚合组成员；如果是，请修改端口聚合组；
- ☞ 镜像目的端口的吞吐量小于镜像源端口吞吐量的总和，目的端口无法完全复制源端口的流量；请减少源端口的个数或复制单向的流量，或者选择吞吐量更大的端口作为目的端口。
- ☞ 在源交换机和中间交换机的RSPAN数据传输链路中，交换机输出方向的Trunk端口的 native vlan是否设置为RSPAN vlan；如果是，请修改Trunk端口的native vlan。
- ☞ 置RSPAN功能后，出口镜像的报文会加上vlan tag，导致反射端口上出现abort错误帧，此时需要修改交换机默认MTU值。

第3章 sFlow 配置

3.1 sFlow 介绍

sFlow（RFC 3176）是基于标准网络导出协议，是由 InMon 公司开发出来的用于监控网络流量信息的协议。其主要操作是由被监视的交换机、路由器把被监控的数据通过采样、统计等操作发送到用于监控的用户端分析器，由分析器对收到的数据进行用户所要求的分析，从而达到监控网络的目的。

一个 sFlow 监控系统包括：sFlow 代理、中央数据收集器、和 sFlow 分析器。SFlow 代理利用采样技术从交换机设备抓取数据。sFlow 数据收集器用来格式化要转发采样的数据统计到 sFlow 分析器，sFlow 分析器对采样数据进行分析并根据分析结果作出相应的处理措施。这里我们的交换机实现的是 sFlow 系统中的代理和中央数据收集器部分。

我们当前实现了针对物理端口的数据采样和统计。

我们实现的采样数据类型针对 IPV4 报文类型、IPv6 报文类型进行处理。其它类型的扩展暂不支持。对于非 IPV4 和 IPv6 的报文，我们按照 RFC3176 的要求，采用统一的头（HEADER）模式，在分析其协议类型的基础上，复制报文的头信息。

InMon 公司发布的 sFlow 协议目前已经更新到了版本 5，由于 RFC3176 实现的是版本 4，而版本之间在结构和报文格式上可能存在一定的不兼容，由于版本 5 还没有成为正式的协议，为与当前的应用软件兼容，我们仍遵照 RFC3176 实现。

3.2 sFlow 配置任务序列

1.配置 sFlow Collector 地址

命令	解释
全局配置模式，端口配置模式	
sflow destination <collector-address> [<collector-port>] no sflow destination	配置 sFlow 分析软件所在主机的 IP 地址和端口号。对于端口来说，如果端口上有配置 IP 地址，则使用端口的配置，否则使用全局的配置。No 命令恢复为默认端口值，删除 IP 地址值。

2.配置 sFlow 代理地址

命令	解释
全局配置模式	
sflow agent-address <collector-address> no sflow agent-address	配置 sFlow 代理使用的源 IP 地址，no 命令删除该地址。

3.配置 sFlow 协议优先级

命令	解释
全局配置模式	
sflow priority <priority-vlaue> no sflow priority	配置 sFlow 从硬件收报文时的优先级, no 命令恢复为默认值。

4.配置 sFlow 复制报文数据头长度

命令	解释
端口配置模式	
sflow header-len <length-vlaue> no sflow header-len	配置 sFlow 在数据采样中复制的报文数据头的长度, no 命令恢复为默认值。

5.配置 sFlow 报文最大允许数据头长度

命令	解释
端口配置模式	
sflow data-len <length-vlaue> no sflow data-len	配置 sFlow 在报文中允许的最大数据长度, no 命令恢复为默认值。

6.配置 sFlow 硬件采样速率

命令	解释
端口配置模式	
sflow rate {input <input-rate> output <output-rate>} no sflow rate [input output]	配置 sFlow 在硬件采样时的采样速率。No 命令删除采样速率值。

7.配置 sFlow 统计采样间隔

命令	解释
端口配置模式	
sflow counter-interval <interval-vlaue> no sflow counter-interval	配置 sFlow 进行统计采样的最大间隔。No 命令删除统计采样间隔值。

8. 配置 sFlow 使用的分析器

命令	解释
全局配置模式	
sflow analyzer sflowtrend no sflow analyzer sflowtrend	配置 sFlow 使用的分析器。no 命令删除 sflow 的分析器。

3.3 sFlow 举例

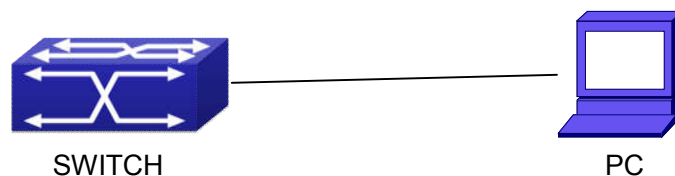


图 3-1 sFlow 配置拓扑图

如图所示, SWITCH 上的端口 1/1 以及 1/2 上启动 sFlow 采样, 假定 PC 上安装了 sFlow 分析器软件, PC 地址为 192.168.1.200, SWITCH 上与 PC 相连的三层接口的地址为 192.168.1.100, SWITCH 上配置了一个地址为 10.1.144.2 的 loopback 接口。以下是 sFlow 的配置

配置步骤如下:

```
switch#config
switch (config)#sflow agent-address 10.1.144.2
switch (config)#sflow destination 192.168.1.200
switch (config)#sflow priority 1
switch (config)#in e1/1
switch (Config-If-Ethernet1/1)#sflow rate input 10000
switch (Config-If-Ethernet1/1)#sflow rate output 10000
switch (Config-If-Ethernet1/1)#sflow counter-interval 20
switch (Config-If-Ethernet1/1)#exit
switch (config)#in e1/2
switch (Config-If-Ethernet1/2)#sflow rate input 20000
switch (Config-If-Ethernet1/2)#sflow rate output 20000
switch (Config-If-Ethernet1/2)#sflow counter-interval 40
```

3.4 sFlow 排错帮助

在配置、使用 sFlow 功能时, 可能会由于物理连接、配置错误等原因导致 sFlow 未能正常运行。因此, 用户应注意以下要点:

- ☞ 应该保证物理连接的正确无误;
- ☞ 保证全局配置模式或者接口配置模式下所配置的sFlow分析器地址是可达的;
- ☞ 如果要求流采样, 必须保证配置了接口下的采样速率;
- ☞ 如果要求统计采样, 必须保证配置了接口下的统计采样间隔。

如果使用检查尝试仍无法解决, 请联系本公司技术服务中心。

第4章 IPFIX 配置

4.1 IPFIX 介绍

IPFIX 全称为 IP Flow Information Export，即 IP 流信息输出，它是由 IETF 根据 Cisco NetFlow Version9 制定的用于网络中流信息测量的标准协议，它使网络中流量统计信息的格式标准化。其主要操作是由被监控的交换机或者路由器根据用户的监控需求，把被监控的数据流进行分类、统计，生成不同的流记录，然后发送到用于监控的用户端的收集器，由收集器对收集到的流记录进行分析和存储，通过记录和分析网络中这些流量的特征，如流量持续时间、流量中报文平均长度等，我们可以了解到当前网络的应用情况，并根据这些信息对网络进行优化，安全检测，流量计费，从而达到监控网络流量的目的。该协议可以工作在任何厂家的网络设备和管理系统平台之上，而且 IPFIX 的数据输出格式是基于模板的，具有很强的可扩展性，如果流量监控的要求发生改变，网络管理员也不必升级网络设备软件或管理工具。

目前网络界基于流(Flow)的分析技术主要有 NetFlow、sFlow 和 IPFIX。NetFlow 是 Cisco 公司独有的技术，它既是一种流量分析协议，又是一种流交换技术，而 IETF 制定的 IPFIX 规范，则是基于 NetFlow V9 设计的，它使得网络中流量统计信息的格式趋于标准化。sFlow 是基于标准网络导出协议，是由 InMon 公司开发出来的用于监控网络流量信息的协议。它采用数据流随机采样技术把采样数据发送到用于监控的用户端分析器，由分析器对收到的数据进行用户所要求的分析，从而达到监控网络的目的。和 IPFIX 相比，sFlow 更像是一种简单的数据采样，更容易支持高速接口，它能提供给分析器更多的报文信息，但报文输出格式是固定的，不能扩展，sFlow 的实时性较强，具备突出的第 2-7 层信息的描述能力。而 IPFIX 可以通过用户的配置把不同的报文流进行分类统计，主要关注报文的头部信息，提供路由器的三层信息。另外，用户可以灵活的配置想要获取的报文内容，同时也可以设定数据输出的模板格式，具有很强的可扩展性。

基于上面的分析，sFlow 主要考虑用于那些对统计结果要求不是特别准确，用户需要关心报文内容的应用环境或者网络流量比较大的环境中。IPFIX 主要用于需要精确统计和对流量进行分类统计的应用环境中，比如需要对服务类型进行分类统计。

IPFIX 是在支持特定芯片的板卡上实现的，和 sFlow 模块不存在互斥关系。因此，交换机或者路由器可以同时支持这两个功能，用户可以根据实际需要来选择不同的流量统计方法。注：16800 机架式设备，只有千兆卡支持。

4.2 IPFIX 基本配置

IPFIX 配置任务序列如下：

1. 配置匹配规则
 - 1) 设置 L2 报文流记录匹配关键字
 - 2) 设置 IPv4 报文流记录匹配关键字
 - 3) 设置 IPv6 报文流记录匹配关键字
 - 4) 设置流记录的非关键字
2. 配置采样规则
3. 配置输出规则
4. 配置监控规则
 - 1) 选择匹配关键字
 - 2) 选择输出地址
 - 3) 选择监控报文类型
 - 4) 设置监控相关参数
5. 将配置应用到端口

1. 配置匹配规则

命令	解释
全局配置模式	
ipfix record <name> no ipfix record <name>	创建新 record，并进入 record 配置模式；本命令的 no 操作为删除指定的 record。
match datalink vlan {id priority} no match datalink vlan {id priority} match datalink mac {destination-address source-address} no match datalink mac {destination-address source-address} match datalink ether-type no match datalink ether-type	设置 L2 报文的流记录关键字，当需要多个关键字时，可进行多次配置。 L2 报文关键字有： vlan-id vlan-priority dst-mac-address src-mac-address ether-type
select {ipv4 ipv6} no select {ipv4 ipv6}	选择流记录匹配关键字的类型。（该命令不配置时，match ip/match ipv4-mask/match ipv6-prefix 命令的配置不生效）

match ip {protocol tos destination-port source-port} no match ip {protocol tos destination-port source-port }	设置 IP 报文（对 IPv4 及 IPv6 报文均生效）的流记录关键字，当需要多个关键字时，可进行多次配置。 该命令设置的报文关键字有： protocol（对 IPv6 而言，是匹配 next-header 字段） tos destination-port source-port
match ipv4-mask destination <mask-length> source <mask-length> no match ipv4-mask	设置匹配 IPv4 报文的源/目的地址掩码长度。（需要与 select ipv4 命令配合使用）
match ipv6-prefix destination <prefix-length> source <prefix-length> no match ipv6-prefix	设置匹配 IPv6 报文的源/目的地址前缀长度。（需要与 select ipv6 命令配合使用）
match ipv6 flow-label no match ipv6 flow-label	设置 IPv6 报文的流关键字为 flow-label。
collect counter {bytes packets} no collect counter {bytes packets} collect timestamp sys-uptime{first last} no collect timestamp sys-uptime{first last}	设置流记录的非关键字，该非关键字用于流信息中提供一些额外信息，但不会产生新流；当需要多个非关键字时，可进行多次配置。 非关键字有： bytes packets sys-uptime first sys-uptime last
description no description	配置描述信息。

2. 配置采样规则

命令	解释
全局配置模式	
ipfix sampler <name> no ipfix sampler <name>	创建新 sampler，并进入 sampler 配置模式；本命令的 no 操作为删除指定的 sampler。
rate <number> no rate	设置采样率为 1/（N+1），每隔 N 个报文采一个。（不区分报文类型）

description	配置描述信息。
no description	

3. 配置输出规则

命令	解释
全局配置模式	
ipfix exporter no ipfix exporter	创建新 exporter，并进入 exporter 配置模式；本命令的 no 操作为删除指定的 exporter。
ipv4 destination <ipv4-address> [source <ipv4-address>] no ipv4 destination ipv6 destination <ipv6-address> [source <ipv6-address>] no ipv6 destination	配置流记录输出的目的地址及源地址，每个 exporter 只能配置一个 IPv4 源/目的地址，或者是一个 IPv6 源/目的地址。
transport {udp tcp sctp} [destination-port <port>] no transport	选择传输协议及传输端口，目前仅支持 UDP 协议。
udp template {timeout-rate <seconds> refresh-rate <packets>} no udp template	配置 UDP 协议下模板重传参数，可以选择以时间或者以发送报文数为间隔单位。
description no description	配置描述信息。

4. 配置监控规则

命令	解释
全局配置模式	
ipfix monitor <name> no ipfix monitor <name>	创建新 monitor，进入 monitor 配置模式；本命令的 no 操作为删除指定的 monitor。
record {<name> default-set [ipv4] [ipv6] [I2] [ipv4-ipv6] [ipv4-I2] [ipv6-I2]} no record	选择监控报文的关键字，可以配置使用步骤 1 所创建的 record 或者是预设的基本流关键字。
exporter <name> no exporter <name>	选择流记录输出地址，对应于步骤 3 所创建的 exporter。
set packet-type {ipv4 ipv6 I2} no set packet-type {ipv4 ipv6 I2}	配置需要监控的报文类型，若需要监控多种报文，可进行多次配置。

deal {non-discard discard all} no deal	配置是否需要监控被标记为丢弃的报文。
cache {entries <entries> timeout {active <active- time> inactive <inactive- time>}} type {normal tcp-end-detect}} no cache {entries <entries> timeout {active <active- time> inactive <inactive- time>}} type {normal tcp-end-detect}}	配置流记录的输出参数，其中包括 cache 中最大流记录存储数，记录输出方式，老化时间及活动时间。
description no description	配置描述信息。

5. 将配置应用到端口

命令	解释
特权模式	
ipfix apply monitor <monitor-name> [sampler <sampler-name>] {input output} no ipfix apply monitor <monitor-name> [sampler <sampler-name>] {input output}	将 ipfix monitor 及 sampler 功能应用于端口，对于每个端口，输入和输出方向都只能设置一个 ipfix monitor。

4.3 IPFIX 举例

案例：

IPFIX 的一个应用是基于使用的计费。IPFIX 记录可以精确到目的 IP、协议类型和端口号等字段，它可以为应用报告提供更详细的测量结果。如下图所示，交换机需要在端口 1/1 上监控某个用户在差分服务网络中的单一流量，需要监控如下信息：

- IPv4 源地址: 4 字节
- IPv4 目的地址: 4 字节
- TOS(DSCP+ECN): 1 个字节

还需要报告通信量结果，这样，要使用流字节数（4 字节）作为输出记录的非关键字。最后将该记录信息输出到 server 服务器。

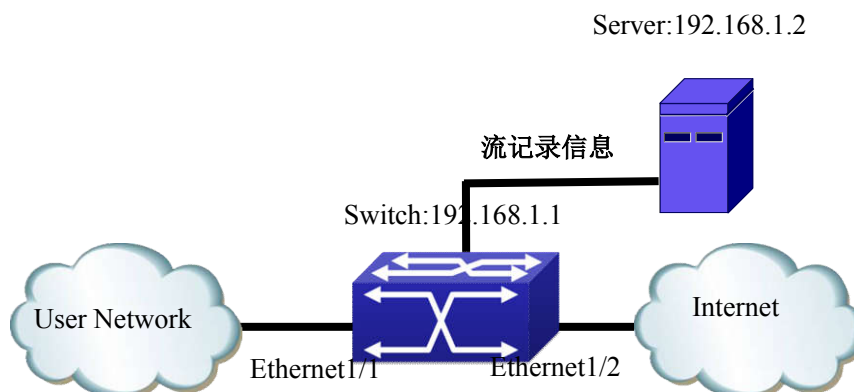


图 4-1 IPFIX 配置

为实现此应用，需按以下方式进行配置：

Switch 的配置(此时无须进行采样规则的配置)：

(1)匹配规则：匹配报文的 IPv4 源地址、IPv4 目的地址和 TOS 字段，流的字节数作为非关键字。

```
Switch(config)#ipfix record my-record
```

```
Switch(config-ipfix-record)#select ipv4
```

```
Switch(config-ipfix-record)#match ipv4-mask destination 32 source 32
```

```
Switch(config-ipfix-record)#match ip tos
```

```
Switch(config-ipfix-record)#collect counter bytes
```

```
Switch(config-ipfix-record)#exit
```

(2)输出规则：输出目的地址为 192.168.1.2，源地址为 192.168.1.1。

```
Switch(config)#ipfix exporter my-exporter
```

```
Switch(config-ipfix-exporter)#ipv4 destination 192.168.1.2 source 192.168.1.1
```

```
Switch(config-ipfix-exporter)#exit
```

(3)监控规则：监控 ipv4 报文，选择关键字及输出地址为步骤 1 和 2 的配置，其他参数使用默认设置即可。

```
Switch(config)#ipfix monitor my-monitor
```

```
Switch(config-ipfix-monitor)#set packet-type ipv4
```

```
Switch(config-ipfix-monitor)#record my-record
```

```
Switch(config-ipfix-monitor)#exporter my-exporter
```

```
Switch(config-ipfix-monitor)#exit
```

(4)将配置应用到端口 1/1。

```
Switch(config)#interface ethernet1/1
```

```
Switch(config-if-ethernet1/1)#ipfix apply monitor my-monitor input
```

```
Switch(config-if-ethernet1/1)#ipfix apply monitor my-monitor output
```

```
Switch(config-if-ethernet1/1)#exit
```

4.4 IPFIX 排错帮助

当在使用 IPFIX 过程中遇到问题，请检查是否是如下原因：

- ☞ 交换机是否正确配置了监控规则，请确保关键字及监控报文类型配置的正确。
- ☞ 请确保交换机与输出目的地址之间的连通性以及所使用的流收集工具(或计费软件)支持 IPFIX 功能。
- ☞ 交换机 IPFIX 功能是否正常，可通过 `debug ipfix monitor` 及 `debug ipfix exporter` 观察交换机能否正确处理及发送相关 IPFIX 报文。

第5章 ERSPAN 配置

5.1 ERSPAN 简介

ERSPAN (Encapsulated Remote Switched Port Analyzer, 密封式远程交换端口分析), 突破了镜像源和目的端口必须处于同一交换机的限制, 使镜像源端口和镜像目的端口可以在不同的网络设备上, 从而方便网管人员对远程交换机设备进行管理。与传统的 RSPAN 相比配置更简单, 使被镜像到的端口流量在指定隧道中传输。

需要注意的问题:

1. ERSPAN 镜像的镜像源只能端口镜像, 目前不支持 CPU 镜像和流镜像。
2. 在源交换机和目的交换机的 ERSPAN 数据传输链路中, 必须有一条隧道。
3. 在使用远程镜像时需注意链路的带宽要满足业务流和镜像流量的需要。

名词解释:

ERSPAN(Encapsulated Remote Switched Port Analyzer): 密封式远程交换端口分析。

5.2 ERSPAN 配置任务序列

1. 指定镜像源端口

命令	解释
全局配置模式	
monitor session <session> source {interface <interface-list> {rx tx both}} no monitor session <session> source {interface <interface-list>}	指定镜像源端口; 本命令的 no 操作为删除镜像源端口。

2. 指定镜像目的隧道

命令	解释
全局配置模式	
monitor session <session> destination tunnel <tunnel-number> no monitor session <session> destination tunnel <tunnel-number>	指定镜像目的隧道; 本命令的 no 操作为删除镜像目的隧道。

5.3 ERSPAN 典型案例

在没有 ERSPAN 之前, 网络管理人员需要带着笔记本电脑跑到各个交换机处, 将电脑连接到交换机上, 才能检测网络的状况, 非常不方便。

而有了 ERSPAN 功能之后，管理员只需要在源交换机上配置好隧道，并制定镜像目的隧道，中间交换机配置 OSPF，目的交换机按照普通端口镜像模式配置，就可以实现远程端口分析。

以下是一个应用环境举例：在一个三层网络中，Device A 通过端口 Ethernet 1/1 连接市场部，并通过端口 Ethernet1/2 与 Device B 的端口 Ethernet1/2 相连；Device C 通过端口 Ethernet1/2 连接 Server，并通过端口 Ethernet1/1 与 Device B 的端口 Ethernet1/1 相连。通过配置远程端口镜像，使 Server 可以通过 GRE 隧道穿越三层网络监控所有进、出市场部的报文。组网图如下所示：

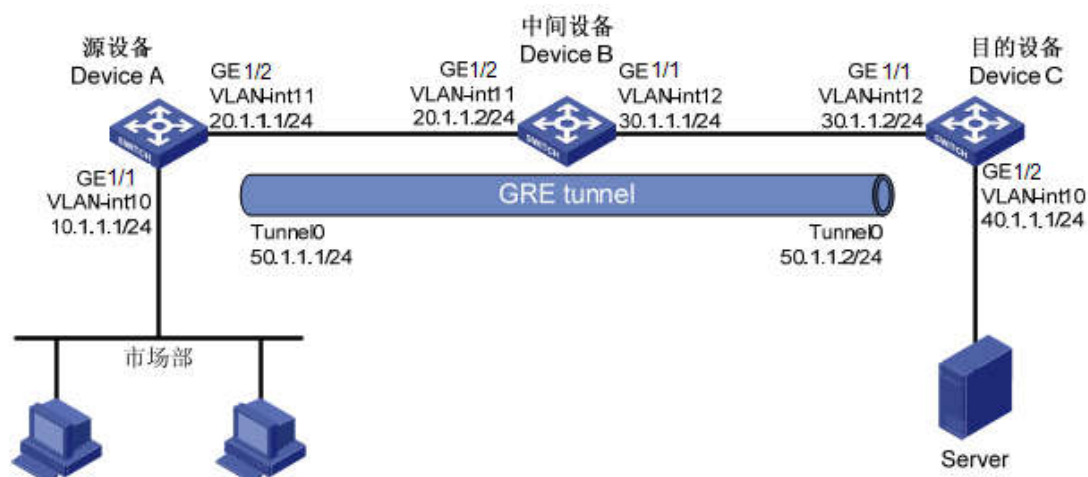


图 5-1 ERSPAN 应用示意图

在配置三层远程端口镜像之前，需完成源设备（Device A）到目的设备（Device C）的 GRE 隧道的配置，并保证 GRE 隧道的正常转发。

三层远程端口镜像的配置需要分别在源设备和目的设备上。分别在源设备（Device A）和目的设备（Device C）上配置源端口和目的端口，不同的是：在 Device A 上，需要将源端口指定为待监控的端口，目的端口指定为 Tunnel 接口；在 Device C 上，需要将源端口指定为 Tunnel 接口对应的物理端口，目的端口指定为连接数据监测设备的端口。

(1) 配置 IP 地址

请按照组网图所示配置 VLAN，并将相应端口加入 VLAN，配置各接口的 IP 地址和子网掩码，具体配置过程略。

(2) 配置源交换机 Device A

创建接口 Tunnel1，并为其配置 IP 地址和掩码。

```
SwitchA(config)#interface tunnel 1
```

```
SwitchA(config-if-tunnel1)# tunnel mode gre ip
```

```
SwitchA (config-if-tunnel1)#ip address 50.1.1.1 255.255.255.0
```

配置 Tunnel1 接口采用 GRE 隧道模式，并为该接口指定源地址和目的地址。

```
SwitchA(config-if-tunnel1)# tunnel source 10.1.1.1
```

```
SwitchA(config-if-tunnel1)# tunnel destination 40.1.1.1
```

```
SwitchA(config-if-tunnel1)# exit
```

配置 OSPF 协议。

```
SwitchA (config)#router ospf
```

```
SwitchA (config-router)#network 0.0.0.0/0 area 0
```

```
SwitchA (config-router)#exit
```

- ```
配置本地镜像组 4 的源端口为 Ethernet1/1，目的端口为 Tunnel1。
SwitchA(config)#monitor session 4 destination tunnel 1
SwitchA(config)#monitor session 4 source interface ethernet 1/1 both
```
- (3) 配置中间交换机 Device B
- ```
# 配置 OSPF 协议。
SwitchB (config)#router ospf
SwitchB (config-router)#network 0.0.0.0/0 area 0
SwitchB (config-router)#exit
```
- (4) 配置目的交换机 Device C
- ```
创建接口 Tunnel1，并为其配置 IP 地址和掩码。
SwitchC(config)#interface tunnel 1
SwitchC (config-if-tunnel1)# tunnel mode gre ip
SwitchC (config-if-tunnel1)#ip address 50.1.1.2 255.255.255.0
配置 Tunnel1 接口采用 GRE 隧道模式，并为该接口指定源地址和目的地址。
SwitchC (config-if-tunnel1)# tunnel source 40.1.1.1
SwitchC (config-if-tunnel1)# tunnel destination 10.1.1.1
SwitchC (config-if-tunnel1)# exit
配置 OSPF 协议。
SwitchC (config)#router ospf
SwitchC (config-router)#network 0.0.0.0/0 area 0
SwitchC (config-router)#exit
配置本地镜像组 1 的源端口为 Ethernet1/1，目的端口为 Ethernet1/2。
SwitchC (config)#monitor session 1 destination interface ethernet 1/2
SwitchC (config)#monitor session 1 source interface ethernet 1/1 rx
```

## 5.4 ERSPAN 排错帮助

当配置 ERSPAN 功能出现问题时，请检查是否是如下原因：

- ☞ 确认 GRE 隧道的配置，并保证 GRE 隧道的正常转发；
- ☞ 镜像目的端口的吞吐量小于镜像源端口吞吐量的总和，目的端口无法完全复制源端口的流量；请减少源端口的个数或复制单向的流量，或者选择吞吐量更大的端口作为目的端口。