Content

Chapter 1 Mirror Configuration

Explanation：

The layer 3 switch in this chapter represents the a general sense of router or wireless controller which is running routing protocol.

1.1 Introduction to Mirror

Mirror functions include port mirror function, CPU mirror function, flow mirror function.

Port mirror refers to the duplication of data frames sent/received on a port to another port. The duplicated port is referred to as mirror source port and the duplicating port is referred to as mirror destination port. A protocol analyzer (such as Sniffer) or a RMON monitor will be connected at mirror destination port to monitor and manage the network, and diagnose the problems in the network.

CPU mirror function means that the switch exactly copies the data frames received or sent by the CPU to a port.

Flow mirror function means that the switch exactly copies the data frames received or by the specified rule of a port to another port. The flow mirror will take effect only the specified rule is permit.

A chassis switch supports at most 4 mirror destination ports, each boardcard allows a source or destination port of a mirror session. At present, each box switch can set many mirror sessions. There is no limitation on mirror source ports, one port or several ports is allowed. When there are more than one source ports, they can be in the same VLAN or in different VLAN. The source port and destination port can be in different VLAN.

1.2 Mirror Configuration Task List

1. Specify mirror destination port
2. Specify mirror source port (CPU)
3. Specify flow mirror source

1. Specify mirror destination port

Command	Explanation
Global mode	

monitor session <*session*> destination interface <*interface-number*> **no monitor session <*session*> destination interface <*interface-number*>**	Specifies mirror destination port; the no command deletes mirror destination source port.

2. Specify mirror source port（CPU）

Command	Explanation
Global mode	
monitor session <*session*> source {interface <*interface-list*> | cpu [slot <*slotnum*>]} {rx| tx| both} **no monitor session <*session*> source {interface <*interface-list*> | cpu [slot <*slotnum*>]}**	Specifies mirror source port; the no command deletes mirror source port.

3. Specify flow mirror source

Command	Explanation
Global mode	
monitor session <*session*> source {interface <*interface-list*>} access-group <*num*> {rx|tx|both} **no monitor session <*session*> source {interface <*interface-list*>} access-group <*num*>**	Specifies flow mirror source port and apply rule; the no command deletes flow mirror source port.

1.3 Mirror Examples

1. Example:

The requirement of the configurations is shown as below: to monitor at interface 1 the data frames sent out by interface 9 and received from interface 7, sent and received by CPU, and the data frames received by interface 15 and matched by rule 120(The source IP address is 1.2.3.4 and the destination IP address is 5.6.7.8).

Configuration guidelines:

1. Configure interface 1 to be a mirror destination interface.
2. Configure the interface 7 ingress and interface 9 egress to be mirrored source.
3. Configure the CPU as one of the source.

4. Configure access list 120.
5. Configure access 120 to binding interface 15 ingress.

Configuration procedure is as follows:

Switch(config)#monitor session 4 destination interface ethernet 1/0/1
Switch(config)#monitor session 4 source interface ethernet 1/0/7 rx
Switch(config)#monitor session 4 source interface ethernet 1/0/9 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 1/0/15 access-list 120 rx

1.4 Device Mirror Troubleshooting

If problems occur on configuring port mirroring, please check the following first for causes:

- ☞ Whether the mirror destination port is a member of a TRUNK group or not, if yes, modify the TRUNK group.
- ☞ If the throughput of mirror destination port is smaller than the total throughput of mirror source port(s), the destination port will not be able to duplicate all source port traffic; please decrease the number of source ports, duplicate traffic for one direction only or choose a port with greater throughput as the destination port. Mirror destination port can not be pulled into Isolate vlan, or will affect mirror between VLAN.
- ☞ When sending unknown unicast, broadcast and multicast data, it is recommended to set only one session for egress mirror.

Chapter 2 RSPAN Configuration

2.1 Introduction to RSPAN

Port mirroring refers to the duplication of data frames sent/received on a port to another port. The duplicated port is referred to as mirror source port and the duplicating port is referred to as mirror destination port. It is more convenience for network administrator to monitor and manage the network and diagnostic after the mirroring function achieved. But it only used for such instance that the mirror source port and the mirror destination ports are located in the same switch.

RSPAN (remote switched port analyzer) refers to remote port mirroring. It eliminates the limitation that the source port and the destination port must be located on the same switch. This feature makes it possible for the source port and the destination port to be located on different devices in the network, and facilitates the network administrator to manage remote switches. It can't forward traffic flows on remote mirror VLAN.

There are three types of switches with the RSPAN enabled:

1. Source switch: The switch to which the monitored port belongs. The source switch copies the mirrored traffic flows to the Remote VLAN, and then through Layer 2 forwarding, the mirrored flows are sent to an intermediate switch or destination switch.
2. Intermediate switch: Switches between the source switch and destination switch on the network. Intermediate switch forwards mirrored flows to the next intermediate switch or the destination switch. Circumstances can occur where no intermediate switch is present, if a direct connection exists between the source and destination switches.
3. Destination switch: The switch to which the destination port for remote mirroring belongs. It forwards mirrored flows it received from the Remote VLAN to the monitoring device through the destination port.

When configuring the RSPAN mirroring of the source switch, reflector port mode or destination mirror port mode can be selected. The destination switch will redirect all the data frames in the RSPAN VLAN to the RSPAN destination port. For RSPAN mirroring, normal mode and advanced mode can be chosen, normal is introduced by default and fit the normal user. The advanced mode fit the advanced user.

1. Advanced mode: To redirect data frames in RSPAN VLAN to the RSPAN destination port, the intermediary and destination devices should support the redirection of flow.

2. Normal mode: To configure the RSPAN destination port in the RSPAN VLAN. Thus, datagrams in the RSPAN VLAN will be broadcasted to the destination port. In this mode, the destination port should be in RSPAN VLAN, and the source port should not be configured for broadcasting storm control. TRUNK ports should be configured carefully in order not to forward RSPAN datagrams to external networks. The normal mode has the benefit of easy configuration, and reduced system resources.

To be noticed: Normal mode is introduced by default. When using the normal mode, datagrams with reserved MAC addresses cannot be broadcasted.

For chassis switches, at most 4 mirror destination ports are supported, and source or destination port of one mirror session can be configured on each line card. For box switches, only one mirror session can be configured. The number of the source mirror ports is not limited, and can be one or more. Multiple source ports are not restricted to be in the same VLAN. The destination port and the source ports can be in different VLAN.

For configuration of RSPAN, a dedicated RSPAN VLAN should be configured first for carrying the RSPAN datagrams. The default VLAN, dynamic VLAN, private VLAN, multicast VLAN, and the layer 3 interface enabled VLAN cannot be configured as the RSPAN VLAN. The reflector port must belong to the RSPAN VLAN. The destination port should be connected to the Monitor and the configured as access port or the TRUNK port. The RSPAN reflector port will be working dedicatedly for mirroring, when a port is configured as a reflector port, it will discards all the existing connections to the remote peer, disable configurations related to loopback interfaces, and stop forwarding datagram. Connectivity between the source and destination switch for Remote VLAN, should be made sure by configuration.

To be noticed:

1. Layer 3 interfaces related to RSPAN VLAN should not be configured on the source, intermediate, and the destination switches, or the mirrored datagrams may be discarded.

2. For the source and intermediate switches in the RSPAN connections, the native VLAN of TRUNK port cannot be configured as the RSPAN VLAN, Otherwise the RSPAN tag will be disposed before reaching the destination switches.

3. The source port, in access or trunk mode, should not be added to RSPAN VLAN if advanced RSPAN mode is chosen. When the reflector port is used for a inter-card mirroring of CPU TX data, it must be configured as TRUNK port and allows the RSPAN VLAN data passing, the Native VLAN should not be configured as RSPAN VLAN.

4. When configuring the remote mirroring function, the network bandwidth should be considered in order to carry the network flow and the mirrored flow.

Keywards:

RSPAN: Remote Switched Port Analyzer.

RSPAN VLAN: Dedicated VLAN for RSPAN.

RSPAN Tag: The VLAN tag which is attached to MTP of the RSPAN datagrams.

Reflector Port: The local mirroring port between the RSPAN source and destination ports, which is not directly connected to the intermediate switches.

2.2 RSPAN Configuration Task List

1. Configure RSPAN VLAN
2. Configure mirror source port（cpu）
3. Configure mirror destination port
4. Configure reflector port
5. Configure remote VLAN of mirror group

1. Configure RSPAN VLAN

Command	Explanation
VLAN Configuration Mode	
remote-span **no remote-span**	To configure the specified VLAN as RSPAN VLAN. The no command will remove the configuration of RSPAN VLAN.

2. Configure mirror source port(CPU)

Command	Explanation
Global Mode	
monitor session <*session*> source {interface <*interface-list*> | cpu [slot <*slotnum*>]} {rx| tx| both} **no monitor session <*session*> source {interface <*interface-list*> | cpu [slot <*slotnum*>]}**	To configure mirror source port; The no command deletes the mirror source port.

3. Configure mirror destination port

Command	Explanation
Global Mode	
monitor session <*session*> destination interface <*interface-number*> **no monitor session <*session*>**	To configure mirror destination interface; The no command deletes the mirror destination port.

destination interface *<interface-number>*	

4. Configure reflector port

Command	Explanation
Global Mode	
monitor session <session> reflector-port <interface-number> **no monitor session <session> reflector-port**	To configure the interface to reflector port; The no command deletes the reflector port.

5. Configure remote VLAN of mirror group

Command	Explanation
Global Mode	
monitor session *<session>* **remote vlan *<vid>*** **no monitor session <session> remote vlan**	To configure remote VLAN of mirror group, the no command deletes the remote VLAN of mirror group.

2.3 Typical Examples of RSPAN

Before RSPAN is invented, network administrators had to connect their PCs directly to the switches, in order to check the statistics of the network.

However, with the help of RSPAN, the network administrators can configure and supervise the switches remotely, which brings more efficiency. The figure below shows a sample application of RSPAN.

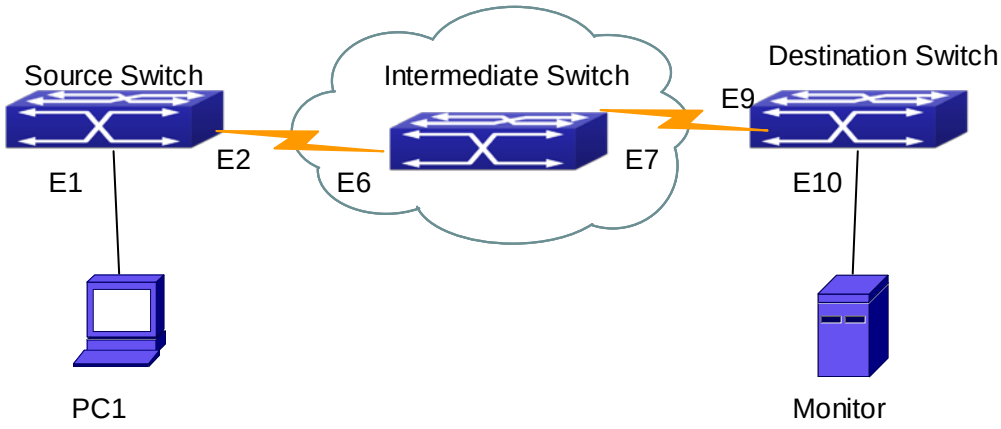

Fig 2-1 RSPAN Application Sample

Two configuration solutions can be chosen for RSPAN: the first is without reflector port, and the other is with reflector port. For the first one, only one fixed port can be connected to the intermediate switch. However, no reflector port has to be configured. This maximizes the usage of witch ports. For the latter one, the port connected to the intermediate switch is not fixed. Datagrams can be broadcasted in the RSPAN VLAN through the loopback, which is much more flexible.

The normal mode configuration is show as below:

Solution 1:

Source switch:

Interface ethernet 1/0/1 is the source port for mirroring.

Interface ethernet 1/0/2 is the destination port which is connected to the intermediate switch.

RSPAN VLAN is 5.

```
Switch(config)#vlan 5
Switch(Config-Vlan5)#remote-span
Switch(Config-Vlan5)#exit
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#switchport mode trunk
Switch(Config-If-Ethernet1/0/2)#exit
Switch(config)#monitor session 1 source interface ethernet1/0/1 rx
Switch(config)#monitor session 1 destination interface ethernet1/0/2
Switch(config)#monitor session 1 remote vlan 5
```

Intermediate switch:

Interface ethernet1/0/6 is the source port which is connected to the source switch.

Interface ethernet1/0/7 is the destination port which is connected to the intermediate switch. The native VLAN of this port cannot be configured as RSPAN VLAN, or the mirrored data may not be carried by the destination switch.

RSPAN VLAN is 5.

```
Switch(config)#vlan 5
Switch(Config-Vlan5)#remote-span
Switch(Config-Vlan5)#exit
Switch(config)#interface ethernet 1/0/6-7
Switch(Config-If-Port-Range)#switchport mode trunk
Switch(Config-If-Port-Range)#exit
```

Destination switch:

Interface ethernet1/0/9 is the source port, which is connected to the source switch.
Interface ethernet1/0/10 is the destination port which is connected to the monitor. This port is required to be configured as an access port, and belong to the RSPAN VLAN.
RSPAN VLAN is 5.

```
Switch(config)#vlan 5
Switch(Config-Vlan5)#remote-span
Switch(Config-Vlan5)#exit
Switch(config)#interface ethernet 1/0/9
Switch(Config-If-Ethernet1/0/9)#switchport mode trunk
Switch(Config-If-Ethernet1/0/9)#exit
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#switchport access vlan 5
Switch(Config-If-Ethernet1/0/10)#exit
```

Solution 2:

Source switch:

Interface ethernet 1/0/1 is the source port.
Interface ethernet 1/0/2 is the TRUNK port, which is connected to the intermediate switch. The native VLAN should not be a RSPAN VLAN.
Interface Ethernet 1/0/3 is a reflector port. The reflector port belongs the RSPAN VLAN, it is access port or TRUNK port of the RSPAN VLAN.
RSPAN VLAN is 5.

```
Switch(config)#vlan 5
Switch(Config-Vlan5)#remote-span
Switch(Config-Vlan5)#exit
Switch(config)#interface ethernet1/0/2
Switch(Config-If-Ethernet1/0/2)#switchport mode trunk
Switch(Config-If-Ethernet1/0/2)#exit
Switch(config)#interface ethernet 1/0/3
Switch(Config-If-Ethernet1/0/3)#switchport mode trunk
Switch(Config-If-Ethernet1/0/3)#exit
Switch(config)#monitor session 1 source interface ethernet1/0/1 rx
Switch(config)#monitor session 1 reflector-port ethernet1/0/3
Switch(config)#monitor session 1 remote vlan 5
```

Intermediate switch:

Interface ethernet1/0/6 is the source port which is connected to the source switch.
Interface ethernet1/0/7 is the destination port which is connected to the destination switch.
The native VLAN of the port should not be configured as RSPAN VLAN, or the mirrored data may not be carried by the destination switch.
RSPAN VLAN is 5.

```
Switch(config)#vlan 5
Switch(Config-Vlan5)#remote-span
Switch(Config-Vlan5)#exit
Switch(config)#interface ethernet 1/0/6-7
Switch(Config-If-Port-Range)#switchport mode trunk
Switch(Config-If-Port-Range)#exit
```

Destination switch:

Interface ethernet1/0/9 is the source port which is connected to the source switch.
Interface ethernet1/0/10 is the destination port which is connected to the monitor. This port is required to be configured as an access port, and belong to the RSPAN VLAN.
RSPAN VLAN is 5.

```
Switch(config)#vlan 5
Switch(Config-Vlan5)#remote-span
Switch(Config-Vlan5)#exit
Switch(config)#interface ethernet 1/0/9
Switch(Config-If-Ethernet1/0/9)#switchport mode trunk
Switch(Config-If-Ethernet1/0/9)#exit
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#switchport access vlan 5
Switch(Config-If-Ethernet1/0/10)#exit
```

2.4 RSPAN Troubleshooting

Due to the following reasons, RSPAN may not function:

- ☞ Whether the destination mirror port is a member of the Port-channel group. If so, please change the Port-channel group configuration;
- ☞ The throughput the destination port is less than the total throughput of the source mirror ports. If so, the destination cannot catch all the datagrams from every source

ports. To solve the problem, please reduce the number of the source ports, or mirror only single direction data flow, or choose some other port with higher capacity as the destination port.

- ☞ Between the source switch and the intermediate switch, whether the native VLAN of the TRUNK ports is configured as RSPAN VLAN. If so, please change the native VLAN for the TRUNK ports.
- ☞ After configured RSPAN, the vlan tag will be added on the packet of the egress mirror. It will cause the abort error frame on the reflection port, so the default MTU value of the switch should be modified.

.

Chapter 3 sFlow Configuration

3.1 Introduction to sFlow

The sFlow (RFC 3176) is a protocol based on standard network export and used on monitoring the network traffic information developed by the InMon Company. The monitored switch or router sends date to the client analyzer through its main operations such as sampling and statistic, then the analyzer will analyze according to the user requirements so to monitor the network.

A sFlow monitor system includes: sFlow proxy, central data collector and sFlow analyzer. The sFlow proxy collects data from the switch using sampling technology. The sFlow collector is for formatting the sample data statistic which is to be forwarded to the sFlow analyzer which will analyze the sample data and perform corresponding measure according to the result. Our switch here acts as the proxy and central data collector in the sFlow system.

We have achieved data sampling and statistic targeting physical port.

Our data sample includes the IPv4 and IPv6 packets. Extensions of other types are not supported so far. As for non IPv4 and IPv6 packet, the unify HEADER mode will be adopted following the requirements in RFC3176, copying the head information of the packet based on analyzing the type of its protocol.

The latest sFlow protocol presented by InMon Company is the version 5. Since it is the version 4 which is realized in the RFC3176, version conflict might exist in some case such as the structure and the packet format. This is because the version 5 has not become the official protocol, so, in order to be compatible with current applications, we will continue to follow the RFC3176.

3.2 sFlow Configuration Task List

1. Configure sFlow Collector address

Command	Explanation
Global mode and Port Mode	
sflow destination <*collector-address*> [<*collector-port*>] **no sflow destination**	Configure the IP address and port number of the host in which the sFlow analysis software is installed. As for the ports, if IP address is configured on the port, the port configuration will be applied, or else will be

	applied the global configuration. The "**no sflow destination**" command restores to the default port value and deletes the IP address.

2. Configure the sFlow proxy address

Command	Explanation
Global Mode	
sflow agent-address <*collector-address*> **no sflow agent-address**	Configure the source IP address applied by the sFlow proxy; the "no" form of the command deletes this address.

3. Configure the sFlow proxy priority

Command	Explanation
Global Mode	
sflow priority <*priority-vlaue*> **no sflow priority**	Configure the priority when sFlow receives packet from the hardware; the "**no sflow priority**" command restores to the default

4. Configure the packet head length copied by sFlow

Command	Explanation
Port Mode	
sflow header-len <*length-vlaue*> **no sflow header-len**	Configure the length of the packet data head copied in the sFlow data sampling; the "no" form of this command restores to the default value.

5. Configure the max data head length of the sFlow packet

Command	Explanation
Port Mode	
sflow data-len <*length-vlaue*> **no sflow data-len**	Configure the max length of the data packet in sFlow; the "no" form of this command restores to the default.

6. Configure the sampling rate value

Command	Explanation
Port Mode	
sflow rate {input <*input-rate*> | **output <*output-rate* >}** **no sflow rate [input | output]**	Configure the sampling rate when sFlow performing hardware sampling. The "no" command deletes the rate value.

7. Configure the sFlow statistic sampling interval

Command	Explanation
Port Mode	

sflow counter-interval <*interval-vlaue*> **no sflow counter-interval**	Configure the max interval when sFlow performing statistic sampling. The “no” form of this command deletes

8. Configure the analyzer used by sFlow

Command	Explanation
Global Mode	
sflow analyzer sflowtrend **no sflow analyzer sflowtrend**	Configure the analyzer used by sFlow, the no command deletes the analyzer.

3.3 sFlow Examples

Fig 3-1 sFlow configuration topology

As shown in the figure, sFlow sampling is enabled on the port 1/0/1 and 1/0/2 of the switch. Assume the sFlow analysis software is installed on the PC with the address of 192.168.1.200. The address of the layer 3 interface on the SwitchA connected with PC is 192.168.1.100. A loopback interface with the address of 10.1.144.2 is configured on the SwitchA. sFlow configuration is as follows:

Configuration procedure is as follows:

Switch#config
Switch (config)#sflow ageng-address 10.1.144.2
Switch (config)#sflow destination 192.168.1.200
Switch (config)#sflow priority 1
Switch (config)# interface ethernet1/0/1
Switch (Config-If-Ethernet1/0/1)#sflow rate input 10000
Switch (Config-If-Ethernet1/0/1)#sflow rate output 10000
Switch (Config-If-Ethernet1/0/1)#sflow counter-interval 20
Switch (Config-If-Ethernet1/0/1)#exit
Switch (config)# interface ethernet1/0/2
Switch (Config-If-Ethernet1/0/2)#sflow rate input 20000
Switch (Config-If-Ethernet1/0/2)#sflow rate output 20000
Switch (Config-If-Ethernet1/0/2)#sflow counter-interval 40

3.4 sFlow Troubleshooting

In configuring and using sFlow, the sFlow server may fail to run properly due to physical connection failure, wrong configuration, etc. The user should ensure the following:

- ☞ Ensure the physical connection is correct
- ☞ Guarantee the address of the sFlow analyzer configured under global or port mode is accessible.
- ☞ If traffic sampling is required, the sampling rate of the interface must be configured
- ☞ If statistic sampling is required, the statistic sampling interval of the interface must be configured

If the examination remains unsolved, please contact with the technical service center of our company.

Chapter 4 IPFIX Configuration

4.1 Introduction to IPFIX

IPFIX (IP Flow Information Export), basing on the Cisco NetFlow Version9, is a standard protocol set by IETF to measure the flow information of the network, and it makes the format of the traffic statistic information to be standard in the network. The primary operation is that the monitored switches or routers classify and count the monitored data flow according to the monitoring requirement of users, create the different flow records and send them to the collector to be monitored, analyzed and stored. By recording and analyzing the characters of these traffic in the network, such as the flow continuance time, the packet's average length in the traffic, we can get the application status of the current network, and accordingly optimize, check the security, count the traffic for the network to achieve the aim of monitoring the network traffic. IPFIX can work on any network devices and management platforms, and its output data format is based on the template, has the very good extensibility. If the the requirement of the flow monitor is changed, the administrator does not need to upgrade the network device software or the management tool.

At present, the Flow Analysis techniques include mostly NetFlow, sFlow and IPFIX. NetFlow is Cisco Company's technique, it is a flow analysis protocol and a flow exchange technique, and IETF set the IPFIX standard based on NetFlow V9, it enables the standardization of the flow statistic information format in the network. sFlow is based on the standard network output protocol and developed by InMon company to monitor the network flow information. It adopts the data flow sampling technique to send the sampling data to the client analyzer which is used to monitor. Then the analyzer analyzes the received data for users to achieve the aim of monitoring the network. Compared with IPFIX, sFlow is a simple data sampling and supports the high speed interface easily. It provides more packet information for the analyzer, but the packet output format is fixed and not extensible. The real time ability of sFlow is better than IPFIX and it has the prominent description ablility of the information of the second to the seventh layer. However, IPFIX can classify and count the different packets by user's configuration, it adverts the head information of the packets mostly and provides the layer 3 information of the routers. In addition, the user can neatly configure the packet's contents which will be obtained, set the template format of the output data and has the good extensibility.

Based on the above analysis, sFlow is mostly used in the application environment of which the statistic results are not required very exactly, users should concern the packet

contents or the bigger network traffic. IPFIX is used in the application environment which needs to count exactly, classify and count the traffic, for example classify and count the service types.

IPFIX is implemented on the card which supports the specific chip, and it is not mutually exclusive to the sFlow module. Therefore, the switch or the router can support two functions at the same time, and the user can select different traffic statistic methods according to the actual requirement.

4.2 IPFIX Basic Configuration

IPFIX Configuration Task List:

1. Configure the match rules
    1) Configure the matching keywords of the flow records for L2 packets
    2) Configure the matching keywords of the flow records for IPv4 packets
    3) Configure the matching keywords of the flow records for IPv6 packets
    4) Configure the non-keyword of the flow records
2. Configure the sampling rules
3. Configure the output rules
4. Configure the monitor rules
    1) Select the matching keyword
    2) Select the output address
    3) Select the type of the monitoring packets
    4) Set the monitored parameters
5. Apply the configuration to the port

1. Configure the match rules

Command	Explanation
Global Mode	
ipfix record <name> **no ipfix record <name>**	Create new record and enter the record configuration mode; the no operation of this command deletes the specific 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**	Set the keywords of the flow record for L2 packets. When it needs multi-keywords, configuring many times is available. The keywords of L2 packets: vlan-id vlan-priority dst-mac-address src-mac-address ether-type
select {ipv4 | ipv6} **no select {ipv4 | ipv6}**	Select the type of the matching keywords for the flow records. (When this command is not configured, the configuration of match ip/match ipv4-mask/match ipv6-prefix command does not take effect.)
match ip {protocol | tos | destination-port | source-port} **no match ip {protocol | tos | destination-port | source-port |}**	Set the keywords of flow records for the IP packets (validate IPv4 and IPv6 packets). When it needs multi-keywords, configuring many times is available. The keywords of the packets are set by this command: protocol (match the next-header field for IPv6) tos destination-port source-port
match ipv4-mask destination <mask-length> source <mask-length> **no match ipv4-mask**	Set the mask length of the source/destination address which match the IPv4 packets. (associate with select ipv4 command to use)
match ipv6-prefix destination <prefix-length> source <prefix-length> **no match ipv6-prefix**	Set the prefix length of the source/ destination address which match the IPv6 packets. (associate with select ipv6 command to use)

match ipv6 flow-label **no match ipv6 flow-label**	Set the flow keyword as the flow-lable for IPv6 packets.
collect counter {bytes | packets} **no collect counter {bytes | packets}** **collect timestamp sys-uptime{first | last}** **no collect timestamp sys-uptime{first | last}**	Set the non-keywords of the flow records, these non-keywords are used to provide some extra information for the flow information, but do not create new flow. When the flow records need multi-keywords, configuring many times is available. The non-keywords: bytes packets sys-uptime first sys-uptime last
description **no description**	Configure the description information.

2. Configure the sampling rules

Command	Explanation
Global Mode	
ipfix sampler <name> **no ipfix sampler <name>**	Create new sampler and enter the sampler configuration mode; the no operation of this command deletes the specific sampler.
rate <number> **no rate**	Set the sampling rate to 1/(N+1), N packets sample one (Do not distinguish the type of the packets)
description **no description**	Configure the description information.

3. Configure the output rules

Command	Explanation
Global Mode	

ipfix exporter **no ipfix exporter**	Create new exporter and enter the exporter mode; the no operation of this command deletes the specific exporter.
ipv4 destination <ipv4-address> [source <ipv4-address>] **no ipv4 destination** **ipv6 destination <ipv6-address> [source <ipv6-address>]** **no ipv6 destination**	Configure destination and source addresses of the output for the flow record, each exporter can configure an IPv4 source/ destination address or an IPv6 source/destination address only.
transport {udp | tcp | sctp} [destination-port <port>] **no transport**	Select the transport protocol and the transport port. At present, only the UDP protocol is supported.
udp template {timeout-rate <seconds> | refresh-rate <packets>} **no udp template**	Configure the retransmit parameters of the template under the UDP protocol, select the time or the sending packet number as the interval unit.
description **no description**	Configure the description information.

4. Configure the monitor rules

Command	Explanation
Global Mode	
ipfix monitor <name> **no ipfix monitor <name>**	Create new monitor and enter the monitor mode; the no operation of this command deletes the specific monitor.
record {<name> | default-set [ipv4] | [ipv6] | [l2] | [ipv4-ipv6] | [ipv4-l2] | [ipv6-l2] } **no record**	Select the keyword of the monitoring packets, so as to configure the record which is created by step 1 or the basic flow keyword of setting.
exporter <name> **no exporter <name>**	Select the output address of the flow records, the address corresponds with exporter which is created by step 3.

set packet-type {ipv4 | ipv6 | l2} **no set packet-type {ipv4 | ipv6 | l2}**	Configure the type of the packets which need to be monitored. If it needs to monitor many kinds of packets, configuring many times is available.
deal {non-discard | discard | all} **no deal**	Configure whether monitor the discarded packets which is tagged.
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}}**	Configure the output parameters of the flow records, the parameters include the storage number of the max flow record, the output method of the records, the aging time and the active time in cache.
description **no description**	Configure the description information.

5. Apply the configuration to the port

Command	Explanation
Admin Mode	
ipfix apply monitor <monitor-name> [sampler <sampler-name>] {input | output} **no ipfix apply monitor <monitor-name> [sampler <sampler-name>] {input | output}**	Apply ipfix monitor and sampler functions to the port, both the ingress direction and the egress direction only can set an ipfix monitor for each port.

4.3 Example of IPFIX

Example:

An application of IPFIX is user-based accounting. IPFIX records can be exact as the fields, such as the destination IP, the protocol type and the port ID, etc. And it can provide the detailed measure results for the application report. The figure is as follows, the switch needs to monitor a user's single traffic within DSCP network on the port 1/0/1, the following information need to be monitored:

- IPv4 source address: 4 bytes
- IPv4 destination address: 4 bytes
- TOS (DSCP+ECN): 1 byte

It is required to report the traffic results, therefore, use the number of the flow byte (4 bytes) as the non-keyword of the output record. Finally, this record information is exported to server.

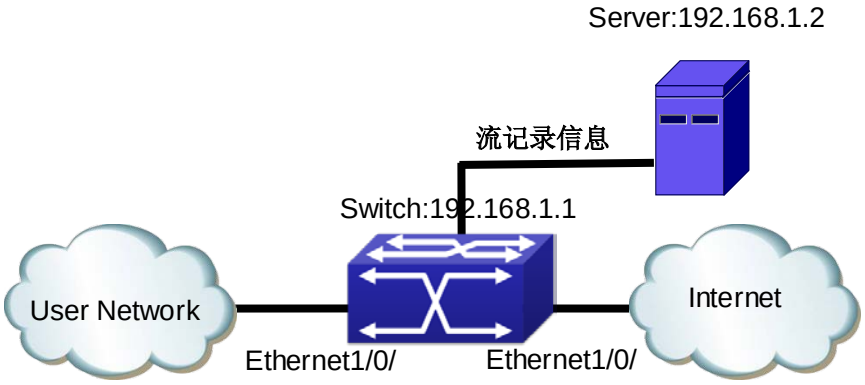

Fig 4-1 IPFIX Configuration

To implement this application, configure according to the following methods:

The configuration of the switch (Do not need to process the configuration of the sampling rules):

(1) The match rules: Match the IPv4 source address, the IPv4 destination address and the TOS field of the packets, the byte number of the flow as the non-keyword.

```
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) The output rules: Export the destination address as 192.168.1.2, the source address as 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) The monitoring rules: Monitor IPv4 packets, select the keywords and export the addresses are the configuration of step 1 and step 2, other parameters use the default setting.

```
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) Apply the configuration to the port 1/0/1.

```
Switch(config)#interface ethernet1/0/1
Switch (config-if-ethernet1/0/1)#ipfix apply monitor my-monitor input
Switch (config-if-ethernet1/0/1)#ipfix apply monitor my-monitor onput
Switch (config-if-ethernet1/0/1)#exit
```

4.4 IPFIX Troubleshooting

If there is any problem happens when using IPFIX, please check whether the problem is caused by the following reasons:

- ☞ Whether the switch configures the monitoring rules correctly, please ensure the keywords and the monitoring packet types are correctly configured.
- ☞ Please ensure the connectivity between the switch and the output destination address, and the flow collection tools (or the accouting software) support IPFIX function.
- ☞ Whether the IPFIX function of the switch is normal, it can use debug ipfix monitor and debug ipfix exporter to check whether the switch process and send the relating IPFIX packets correctly.