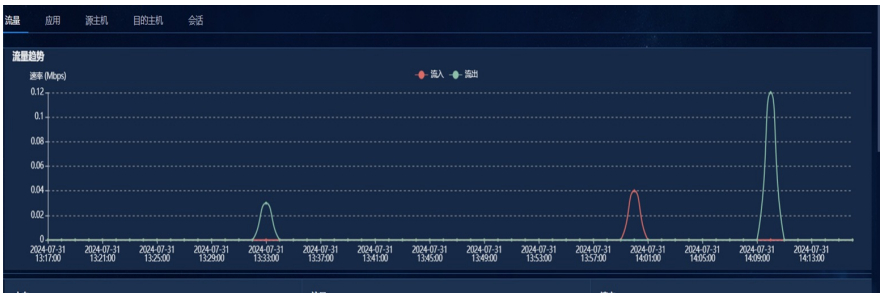
S5554F-EI-D 配置sflow后某终端监控流量异常

sFlow 黄聪琴 2024-08-30 发表

问题描述

现场交换机不支持netstream，需要使用sflow实现网管平台对终端流量的监控，网管平台为UC2.0。

配置sflow后，在网管平台上有一个IP的流量每隔一段时间才能看到有流量，而不是一直能看到流量的实时监控



过程分析

1、结合软件侧排查，结合UC2.0配置sflow的典配，检查配置没问题。
https://www.h3c.com/cn/Service/Document_Software/Document_Center/SDN/Catalog/U-Center/U-Center/Configure/Typical_Configuration_Example/H3C_U_Center_2.0_CE-11548/04/?CHID=1034698
2、在设备侧debugging sflow all，看到设备侧也是有发包的
*Jan 5 06:34:40:166 2013 H3C SFLOW/7/COLLECTOR: **sFlow send a packet:**
Collector ID = 1
Collector address = 192.168.X.X（网管平台地址）
Vrfindex = 0
sFlow datagram version = 5
Agent IP version = 1
Agent IP address = 192.168.Y.Y（设备配置的agent地址）
Sub agent id = 8
Sequence number = 16249
Uptime = 369298000
Sample number = 1
3、在交换机上部署流统，统计异常终端的流量，发现此终端流量较小，十分钟有500个包左右。
而在设备上配置采集的接口5口上来的流量不只这一个终端，sflow配置的采集是每4000个包随机采集一个包，所以可能采集时没有采集到此终端的报文，不连续是正常现象。

```
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 1000
 sflow flow collector 1
 sflow sampling-rate 4000
 sflow counter collector 1
 sflow counter interval 30
 mirroring-group 1 mirroring-port both
#
```

解决方法

将sflow sampling-rate的值改小一些（此设备最小为1000）观察采集到的异常终端的流量不连续的情况是否会好一些。
如果现场想实现实时监控终端的流量，sflow可能没办法很好的实现，其机制是收到了多少个包就采集一个发给网管平台，网管平台根据1秒发了多少个包过来算流量的速率。