MSR系列路由器显示Netstream的报文DIF字段异常

纪合宝 2008-05-28 发表

MSR系列路由器

Netstream的报文DIF字段异常

一、组网：

MSR使能Netstream，使用linux的flow tools对流量进行分析统计。

二、问题描述：

1．客户使用路由器做采集器，使用flow tools对流量进行采集分析，发现netstream时候DIF字段AR与MSR显示结果不一样。

AR的如下，Dif（出接口）有实际序号。

Sif SrcIPaddress Dif DstIPaddress Pr SrcP DstP Pkts Octets

0006 10.67.147.42 0004 70.89.4.57 06 c09d 19 4 166

.....

MSR的如下，Dif 一直为O

Sif SrcIPaddress Dif DstIPaddress Pr SrcP DstP Pkts Octets

0003 1.1.1.2 0000 1.1.1.1 01 0 303 8 1072

0006 10.125.16.214 0000 10.125.16.255 11 8a 8a 1 229

0003 1.1.1.2 0000 1.1.1.1 01 0 800 61 5124

2.与CISCO的Netflow配合发现只能采集入方向的流量。

三、过程分析：

1．Netstream的实现方式是按七元组标识一条流：源ip,目的ip,协议号，源端口，目的端口，TOS,接口，其中的接口是这样记录的:(入的报文)入接口，(出的报文)出接口, 在该情况下：即在同一条流的入接口和出接口分别使能入方向的Netstream和出方向的Netstream时，将这样的Netstream流日志发给部分服务器后，部分类型的服务器例如XLOG，会将该流统计两次，从而导致流量统计不准。为了与这类服务器兼容，做了如下修改：

入接口统计时，不记录出接口；出接口统计时，不记录入接口。

从而在MSR上，该字段不再标记接口，始终为零。

2.Netflow属于思科的流量统计工具，目前流量统计领域并没有RFC标准。我们的Netstream是在cisco Netflow的基础上改进的，增加了“标记流方向”功能(NS_ID)。在Netstream日志报文的日志头的第一个字节用来标记流方向，第二个字节用于标记版本号。但Cisco的日志报文中的前两个字节都是用来标记版本号的，没有标记流方向。v3平台有命令ip netstream format no-direction和思科进行互通。但是目前的v5平台尚无此命令（后续支持）。