

## 组网及说明

SR66-----Server

## 问题描述

现场反馈我们设备（SR66 R7740P15）配置Netstream与第三方服务器（鼎兴达流量分析）对接时，服务器对报文部分字段无法识别，导致流量分析程序不能正常解析数据包。

The image shows a Wireshark packet capture of an MPLS packet. The packet list pane shows several packets of type CFWLM. The packet details pane for packet 11 shows the following fields:

- Field (5/26): IP\_SRC\_ADDR
- Field (6/26): IP\_DST\_ADDR
- Field (7/26): IP\_NEXT\_HOP
- Field (8/26): BGP\_NEXT\_HOP
- Field (9/26): L4\_SRC\_PORT
- Field (10/26): L4\_DST\_PORT
- Field (11/26): PROTOCOL
- Field (12/26): IP\_TOS
- Field (13/26): TCP\_FLAGS
- Field (14/26): MPLS\_TOP\_LABEL\_TYPE
- Field (15/26): INPUT\_SNMP
- Field (16/26): OUTPUT\_SNMP
- Field (17/26): DIRECTION
- Field (18/26): MPLS\_LABEL\_1
- Field (19/26): MPLS\_TOP\_LABEL\_ADDR
- Field (20/26): Unknown(65) - Type: Unknown (65) - Length: 4
- Field (21/26): FLOW\_CLASS
- Field (22/26): SAMPLING\_ALGORITHM
- Field (23/26): Unknown(0) - Type: Unknown (0) - Length: 1
- Field (24/26): SAMPLING\_INTERVAL
- Field (25/26): SRC\_TRAFFIC\_INDEX
- Field (26/26): VRFname

其中Template type 0 与 type 65无法识别。

## 过程分析

### 一、首先检查设备侧配置。

```
# sampler liuliangfenxi mode fixed packet-interval 10
#
ip netstream mpls label-positions 1
ip netstream timeout active 60
ip netstream export version 9 peer-as
ip netstream export host 10.87.xx.xx 2101
ip netstream export source interface LoopBack0
ip netstream export rate 200
#
interface GigabitEthernet3/0/0
ip netstream inbound
ip netstream outbound
ip netstream inbound sampler liuliangfenxi
ip netstream outbound sampler liuliangfenxi
#
```

现场配置选用netstream版本9，并无异常。

### NetStream流输出格式

目前NetStream输出的报文主要有如下版本：

- 版本5：根据七元组产生原始的数据流，不支持聚合流输出，报文格式固定，不易扩展。
- 版本8：支持聚合流输出，报文格式固定，不易扩展。
- 版本9：基于模板方式，模板可在遵循RFC定义的模板格式的前提下自定义。版本9支持聚合流输出，对BGP下一跳信息和MPLS报文的统计输出。

二、查了一下RFC3954 < <https://tools.ietf.org/html/rfc3954#page-18> >和 RFC5102 < <https://tools.ietf.org/html/rfc5102#section-5.1> >

ElementID	Name	Abstract Data Type	Data Type Semantics	Status	Description	Units	Range	References
0	Reserved							

The value field is a numeric identifier for the field type. The following value fields are reserved for proprietary field types: 25, 26, 43 to 45, 51 to 54, and 65 to 69.

Refer to: <https://www.iana.org/assignments/ipfix/ipfix.xhtml>

发现Template 报文中的Type 0 为保留字段，Type 65 为私有字段。故 Wireshark 与第三方的流量分析软件都无法解析。

三、查了一下我们的netstream技术白皮书，没有对我们私有字段的说明。

#### 解决方法

经研发确认：

0: PAD 空白占位符

65: MPLS top label ip mask

第三方服务器增加字段定义后问题解决。