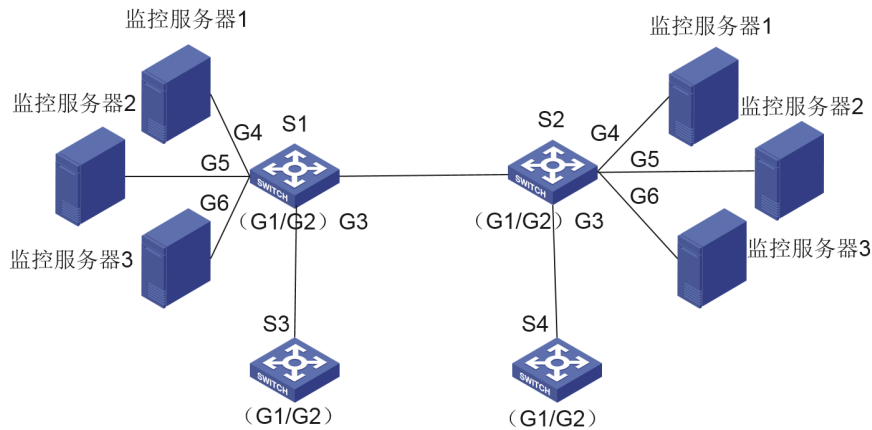


某局点S6520X-54XG-EI-G设备使用TAP功能，进行远程M:N复制的实现流量镜像的配置

镜像 徐猛 2020-03-06 发表

组网及说明



如上述网络拓扑，现场希望实现如下需求：

- (1) S1, S2, S3, S4四台交换机的G1口的流量，全部都能同时镜像到S1和S2连接的监控服务器1和服务器2。
- (2) S1, S2, S3, S4四台交换机的G2口的流量，全部都能同时镜像到S1和S2连接的监控服务器2和服务器3。

现场使用的交换机均为我司的S6520X-54XG-EI-G，该型号设备支持TAP功能的M:N镜像。

配置步骤

现场的需求较为复杂，若需要实现现场的需求，需要在四台设备的G1、G2接口均添加不同的最外层vlan tag（注意，这两个vlan id只能用于此次监控业务，如果使用nest top-most vlan命令给报文封装外层vlan标签，需要注意流量经过的接口需放通外层以及内层的vlan tag）

主要步骤如下：

一：针对S3设备，对不同接口上来的流量，外层加上不同的非业务vlan标签，并进行流量重定向，具体如下：

1.在S3上创建监控组1，监控组1中加入S3-S1的接口

2.针对S3的G1口和G2口上，分别

(1) 在S3上创建流量类1，匹配所有S3-G1口进来的所有流量，创建流行为1，对S3-G1口入方向添加报文的外层VLAN Tag10并重定向镜像至S3-S1口，创建qos tap策略关联流量类1和流行为1，并将该qos tap策略应用在S3-G1口的入方向上。其中流行为1配置如下：

```
traffic behavior 1
nest top-most vlan 10 -----也可以使用remark service-vlan-id vlan-id
redirect monitoring-group 1
```

(2) 在S3上创建流量类2，匹配所有S3-G2口进来的所有流量，创建流行为2，对S3-G2口入方向添加报文的外层VLAN Tag20并重定向镜像至S3-S1口，创建qos tap策略关联流量类2和流行为2，并将该qos tap策略应用在S3-G2口的入方向上。其中流行为2配置如下：

```
traffic behavior 2
nest top-most vlan 20 -----也可以使用remark service-vlan-id vlan-id
redirect monitoring-group 1
```

二：针对S1设备：对S1-G1口和S1-G2口的处理方式和S3类似。在S1-S3口（即S1-G3口）入方向匹配报文最外层vlan-id，转发至对应监控服务器以及对端S2。在S1-S2的入口入方向，识别对端S2发来的镜像流量的vlan标签，并TAP重定向至S1互联的指定监控服务器上。具体如下：

1.在S1上创建监控组1，其中包含G4, G5, 以及S1-S2的口。

在S1上创建监控组2，其中包含G5, G6, 以及S1-S2的口。

在S1上创建监控组3，其中包含G4, G5口

在S1上创建监控组4，其中包含G5, G6口

2.在S1设备的G1, G2口上

(1) S1-G1口入方向调用qos tap策略, 匹配G1口进入的所有流量, 并执行qos tap动作添加报文的外层VLAN Tag10并镜像至监控组1:

traffic behavior 1

nest top-most vlan 10

redirect monitoring-group 1

(2) S1-G2口入方向调用qos tap策略, 匹配G2口进入的所有流量, 并执行qos tap动作添加报文的外层VLAN Tag20并镜像至监控组2:

traffic behavior 1

nest top-most vlan 20

redirect monitoring-group 2

3.S1-S3口 (即S1-G3口) 入方向匹配最外层的vlan-id, 并分别镜像至监控组1 (G4、G5、S1-S2口)、监控组2 (G5、G6、S1-S2口)

在S1-S3口的入方向调用的qos tap policy里, 包含两个cb对:

Tap policy: tap

Classifier: 1

Operator: AND

Rule(s) :

If-match service-vlan-id 10

Behavior: 1

Redirecting:

Redirect to the monitoring group: 1

Classifier: 2

Operator: AND

Rule(s) :

If-match service-vlan-id 20

Behavior: 2

Redirecting:

Redirect to the monitoring group: 2

4.在S1-S2入方向, 匹配对端S2转发来的流量最外层的vlan-id, 并分别镜像至S1设备上的监控组3 (G4、G5)、监控组4 (G5、G6)

在S1-S2口的入方向调用的qos tap policy里, 包含两个cb对:

Tap policy: tap

Classifier: 1

Operator: AND

Rule(s) :

If-match service-vlan-id 10

Behavior: 1

Redirecting:

Redirect to the monitoring group: 3

Classifier: 2

Operator: AND

Rule(s) :

If-match service-vlan-id 20

Behavior: 2

Redirecting:

Redirect to the monitoring group: 4

S2\S4以此类推

配置关键点

在该配置中, 需要在接口上, 调用qos tap策略, 对接口上进入的流量同时进行打标签, 以及重定向的动作。同时由于现场的需求较为复杂, 涉及的接口较多, 需要配置多个监控接口组, 需要注意其中的调用逻辑。