E1线路上MPLS VPN下的丢包分析案例

张瑞 2007-08-08 发表

E1线路上MPLS VPN是否丢包分析案例

1. 问题现象：

某网络西安至灵武节点前置机之间应用软件通讯异常，现象为西安侧的前置机发送request报文，灵武侧设备无应答或偶尔应答，应答的概率约为10%，即西安侧发10个request请求，灵武侧只给一个应答。 用户通过修改应用软件后，灵武侧自动周期向西安侧发送数据，该数据能够正常被西安的前置机接收，没有丢包现象。因此用户怀疑是否request请求在通过MPLS VPN隧道时发生了丢包。

2. 组网图：

如下图所示，西安与银川的两台NE16之间通过E1线路互联，西安双网卡前置机与灵武侧Linux终端前置机的业务数据通过两台路由器之间建立的MPLS VPN隧道进行互联。

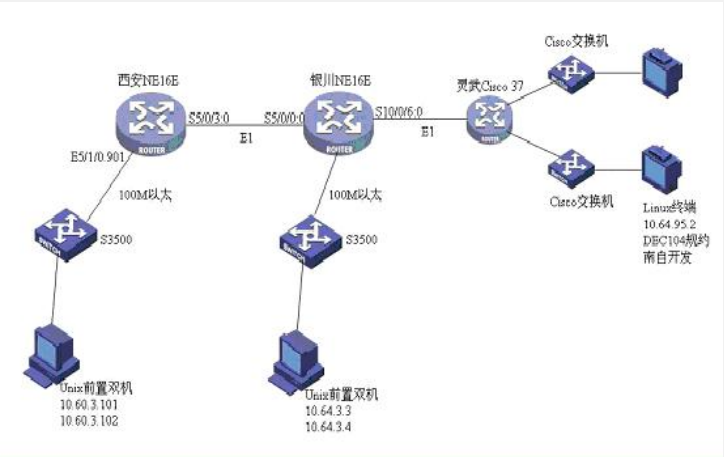

图1 – 某网络西安至灵武节点拓扑示意

3. 问题定位过程：

3.1 测试思路：

方案1：通过观察前置机的收发包数量。因西安的前置机同时与所有分支进行通讯，所以仅通过网卡的收发包数量无法准确获知发往某一目的地包的数量，因此该方案不是最佳方案。

方案2：通过对西安到灵武前置机报文经过各个NE16E端口数量的统计来确定是否存在丢包。具体的说就是从西安节点入接口进入的包是否等于从西安节点发出的包；从银川节点进入的包是否等于从银川节点发出的包。

3.2 技术难点：

西安到银川是通过E1线路互联，因此不能直接抓包，最后通过对目标数据 “着色” 区分后进行统计分析。

3.3 测试过程：

步骤一：分析业务流的特点，西安前置机同时与西北各个网点的前置机进行通信，进行 业务数据的请求与应答。虽然西安两台前置机都是双网卡，但是与灵武进行通 信的只有两块网卡，即互访IP地址对应关系为：

	IP地址
西安前置机	10.60.3.101
	10.60.3.102
灵武前置机	10.64.95.2

为了统计收发包的数量，制定了对应以上地址的acl策略如下：

acl number 3001

rule 5 permit ip vpn-instance vpn-rt source 10.60.3.101 0 destination 10.64.95.2 0

rule 10 permit ip vpn-instance vpn-rt source 10.60.3.102 0 destination 10.64.95.2 0

步骤二：在西安路由器上增加以下配置，目的是对符合acl 3001的包修改其mpls-exp 值 为3，以区别于其它报文，然后进行统计：

//定义类remark

[7.25]traffic classifier remark

//如果符合acl 3001
[7.25-classifier-remark]if-match acl 3001
//定义流行为remark
[7.25]traffic behavior remark
//标记报文MPLS的EXP字段值为3（默认为4，6）
[7.25-behavior-remark]remark mpls-exp 3
//将类与行为进行关联
[7.25]traffic policy remark
[7.25-trafficpolicy-remark]classifier remark behavior remark
//将策略应用到NE16的入接口
[7.25]int Ethernet 5/1/0.901
[7.25-Ethernet5/1/0.901]traffic-policy remark inbound

[7.25]traffic classifier exp3
[7.25-classifier-exp3]if-match mpls-exp 3
[7.25]traffic behavior exp3
//增加ef队列的带宽，原配置为200，此处担心是由于突发流量过大引起丢包，故将带宽放到最大已排除带宽问题代理的影响。
[7.25-behavior-exp3]queue ef bandwidth 1400
[7.25]traffic policy p_vpn_rt
[7.25-trafficpolicy-p_vpn_rt]classifier exp3 behavior exp3
步骤三：
以上配置配完之后分别用命令行
display traffic policy interface Ethernet 5/1/0.901 //西安节点入接口
display traffic policy interface Serial 5/0/3:0 //西安节点出接口
轮番查看，看两个的统计计数是否一致，判断在此设备上是否有丢包
注意数据包入接口interface Ethernet 5/1/0.901 下主要查看以下参数：
Classifier: remark
Matched : 824/36384 (Packets/Bytes)
Operator: AND
Rule(s) : if-match acl 3001
Behavior: remark
Marking:
Remark MPLS EXP 3
Remarked: 824 (Packets)
数据包出接口interface s5/0/3:0下主要查看以下参数：
Classifier: exp3
Matched : 27/1314 (Packets/Bytes)
Operator: AND
Rule(s) : if-match mpls-exp 3
Behavior: exp3
Expedited Forwarding:
Bandwidth 1300 (Kbps), CBS 32500 (Bytes)
Matched : 0/0 (Packets/Bytes)
Enqueued : 0/0 (Packets/Bytes)
Discarded: 0/0 (Packets/Bytes)
步骤四：
类似的在银川NE16E上做类似配置：
[7.25-classifier-car]if-match mpls-exp 3
[7.25]traffic behavior car
[7.25-behavior-car]car cir 50000000 green pass red pass
[7.25]traffic policy car
[7.25-trafficpolicy-car]classifier car behavior car
将此策略分别应用到下面两个串口上
[7.25]int Serial 5/0/0:0
[7.25-Serial5/0/0:0]traffic-policy car inbound
两个串口的方向是不一样的
[7.25]int Serial 10/0/6:0
[7.25-Serial10/0/6:0]traffic-policy car outbound
然后仿照西安节点的做法，周期查看银川节点NE16E接口的收发包数。
步骤五：
间隔10s各接口收发包统计结果（取部分数据），下表部分采样数据显示接口收发包稳定增长，西安、银川各出入口成等差数列分布，除去因人为输入命令造成的微小误差外，西安与银川数据包的增长数量基本相等：

西安共发出包数：

0 + 13 + … + 5 + 9 = 106

银川共收到包数：

0 + 12 + … + 4 + 9 = 108

序号	西安入口 S5/0/3:0	包增长数	西安出口 E5/1/0.901	出入差值	银川入口 S5/0/0:0	包增长数	银川出口 S10/0/6:0	出入差值
1	14	**0**	14	0	19	**0**	19	0
2	27	**13**	27	0	31	**12**	31	0
3	35	**8**	36	1	42	**11**	42	0
4	47	**12**	47	0	55	**13**	55	0
5	53	**6**	53	0	60	**5**	60	0
6	59	**6**	59	0	66	**6**	66	0
7	65	**6**	65	0	72	**6**	72	0
8	70	**5**	70	0	77	**5**	78	1
9	78	**8**	78	0	84	**7**	84	0
10	83	**5**	83	0	90	**6**	90	0
11	88	**5**	88	0	95	**5**	95	0
12	98	**10**	98	0	104	**9**	104	0
13	103	**5**	103	0	110	**6**	110	0
14	106	**3**	106	0	114	**4**	114	0
15	111	**5**	111	0	118	**4**	118	0
16	120	**9**	120	0	127	**9**	127	0
合计	1157	**106**	1158	1	1264	**108**	1265	1

综合以上因素：

1. 各入接口包数与出接口包数基本相同
2. 160s内西安与银川总包增长数趋于相同（该总数因为是人为显示，先查看西安设备，再查看银川设备，同时时间上有前后的误差，所以总数有差别，从长期5分钟，1小时来看基本相同）

4. 结论：

通过以上数据分析得出西安的NE16E与银川的NE16E通过MPLS VPN在对西安到灵武数据的传输中没有丢包。

2007-08-01