某局点 CR16K-F 配置646端口防攻击后LDP邻居中断

LDP packet-filter 林宇阳 2023-06-26 发表

组网及说明

无特定组网，CR16K-F设备与上行设备建立LDP邻居关系。

告警信息

LDP邻居超时断开：

```
%Jun  9 00:16:03:543 2023                                    LDP/4/LDP_SESSION_CHG: Session (      0.1:0, public instance) is down (hello hold timer expired). (LocalTransportAddr=      100.54, PeerTransportA
ddr=      0.1, SessionRole=Active, SessionUpTime=0366:22:19, KeepaliveTime=45s, KeepaliveSentCount=2113517, KeepaliveRcvdCount=2130943, GracefulRestart=Off, SocketID=45, WaitSendMsg=0, CPUUsage=2%, MemoryS
tate=Normal).
%Jun  9 00:16:03:542 2023 HALUY-PA-CMNET-RTO1-fenghuajie LDP/5/LDP_ADJACENCY_DOWN: ADJ(      0.1:0, public instance, RAGG64) is down (hello hold timer expired). (Type=Link, SourceAddr=      .6.141, Destinat
ionAddr=224.0.0.2, TransportAddr=      .0.1, ADJUpTime=0366:22:19, HelloHoldTime=15s, HelloSentCount=6340553, HelloRcvdCount=6603759)
```

问题描述

客户网络有646端口防攻击需求，需要增加阻断非邻居设备的646端口号配置。

但现场实际操作后，发现与对端设备的LDP邻居超时断开，回滚配置后LDP邻居恢复。

过程分析

现场原配置关键配置如下，修改配置前LDP邻居正常。

```
mpls lsr-id Y.Y.100.54  //本地loopback地址
#
interface LoopBack0
 description TO-manage
 ip address Y.Y.100.54 255.255.255.255
#
acl advanced 3502
rule 5 permit ip source X.X.0.1 0     //LDP邻居loopback地址
rule 10 deny tcp destination Y.Y.100.54 0 destination-port eq 646
rule 15 deny udp destination Y.Y.100.54 0 destination-port eq 646
rule 9999 permit ip
#
 packet-filter 3502 global inbound
```

发生故障时，现场将ACL 3502的rule 10和rule 15改为如下规则：

```
rule 10 deny tcp destination-port eq 646
rule 15 deny udp destination-port eg 646
```

修改后，LDP邻居断开，原因为hello保活超时。

处理本问题需要先了解LDP协议的交互和保活机制：

1、路由器在接口使能LDP后，会定时发送源地址是接口IP，目的地址为224.0.0.2的组播hello报文，用于发现邻居设备。

2、两台路由器hello交互完成互相发现后，获知了对端的MPLS Lsr-id，然后就可以进行LSR-id地址的TCP协商建立正式的LDP邻居关系，交互标签数据

3、邻居建立后，LDP有双重保活检查机制：①TCP连接自带的keepalive保活；②接口定时发送组播hello报文保活。二者任一出现问题都会导致LDP邻居关系断开

4、LDP的TCP连接使用TCP 646端口，接口hello组播报文使用UDP 646端口。

现场ACL 3502中仅在rule 5放通了邻居的loopback地址为源的报文，所以修改rule 15后，对端发送的接口hello组播报文会被packet-filter直接匹配阻断，所以本端路由器在数个周期不能收到LDP hello报文后断开了LDP邻接关系。

解决方法

在ACL 3502中增加如下rule 6，提前放通对端接口IP为源的报文即可。

```
rule 6 permit udp source M.M.M.141 0      //对端接口IP
```