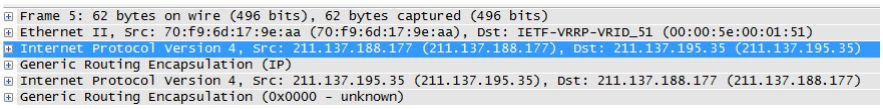
M9000与对端建立GRE隧道并开启keepalive功能异常问题处理案例

GRE 沈博文 2016-01-29 发表

在M9000对端配置gre keepalive后，M9000上tunnel接口协议和物理状态持续为up，但是对端的tunnel协议状态会出现震荡，当修改tunnel参数或者对tunnel口进行手工重启后，可以临时恢复，但是会引起多个对端设备同时出现接口Up/down的情况。

Gre keepalive的请求包封装格式如下图所示，在GRE外层IP头内部封装一个只有源目IP相反的IP报文：



在M9000接受并解封装keepalive报文后，在设备上针对报文会建立两条方向相反的转发表项，同样如果M9K上配置了keepalive后，发送报文时也具有相同情况，因此在设备上转发表项就会出现从A地址到B地址的入方向转发表和出方向转发表同时存在的可能。

在转发表中有安全域参数，例如对于防火墙接收到对端发送的keepalive报文，建立的转发表项是从tunnel接口所在GRE域作为入域，转发到local本地域。

但是现场出现问题时分为如下两种情况。

1) M9000侧不配置keepalive，对端配置keepalive，此时对端tunnel接口协议状态会出现震荡，针对这种情况，分析如下：

M9000侧接收到keepalive报文，当解封装报文的同时，发生arp重新学习，原来的表项因arp重新学习而失效，重新建立转发表项，在软件实现上，此时M9000会把表项建立的入安全区域认为reth冗余口所在安全区域，出安全区域为tunnel所在的安全区域。

2) M9000侧配置keepalive，同时对端也配置keepalive，此时对端tunnel接口协议状态会出现震荡，针对这种情况，分析如下

当GGSN侧发送的keepalive报文被防火墙收到，M9000发送keepalive报文时，M9000同时建立表项，会出现解封装后回复的报文与发送报文内容一致，但ip地址方向相反，表项建立会检测到冲突，重新建立表项，在软件实现上，此时M9000会把入安全区域认为是reth冗余口所在安全区域，出安全区域是tunnel所在的安全区域。

另外一个问题现象，当修改tunnel参数或者重启某个tunnel接口时，对端多台设备会出现同时有多个tunnel接口up/down的情况，分析如下：

在修改tunnel参数或者改变接口状态，会触发重新建立快速转发表项，在软件实现上，此时M9000会把表项建立的入安全区域认为reth冗余口所在安全区域，出安全区域为tunnel所在的安全区域。

放通tunnel接口所在区域和流量实际出口所在区域间的gre keepalive报文。