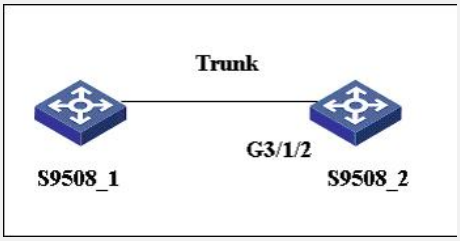
S9500交换机双机Trunk互联组网下anti-attack arp防攻击命令导致误告警的解决方法

王霖 2009-02-07 发表

S9500交换机双机Trunk互联组网下anti-attack arp防攻击命令导致误告警的解决方法

一、 组网：



两台设备双机组网，中间互联链路为trunk

两台S95交换机互联接口为G3/1/2，在S9508_2上该端口的配置如下：

interface GigabitEthernet3/1/2

port link-type trunk

port trunk permit vlan 1 to 500 1000

互联端口之间有多个VLAN二层互联，并启用了三层接口，数量约有40个。

二、 问题描述：

在S9508_2的log日志中，以及console控制台上不定期打印信息检测到ARP攻击，但实际并未发生ARP攻击：

%Dec 26 08:42:12 2008 S9508_2 DIAGCLI/5/LOG_WARN:Slot=3;

Detect ARP attack from MAC 000f-e2a4-e36c, VLAN: 26, GigabitEthernet3/1/2 !

其中提示攻击的MAC地址为对端（S9508_1）VLAN三层接口虚MAC。

三、 过程分析：

S9500系列交换机拥有ARP防攻击功能，而其触发门限值默认为30pps，即1秒钟收到某固定源MAC地址的ARP报文超过30个，则认为存在攻击。

S9500交换机每个的VLAN虚接口的MAC都相同，所以每个VLAN内发送的ARP请求源地址都是相同的，由于这个特点会在某些组网下触发对端的ARP防攻击功能告警或阻断。在前面图片中描述的双机Trunk互联组网中，当由于某些原因S9508_1上ARP表清空（如STP拓扑变化），需要重新获得对端ARP信息时，S9508_1便会在trunk允许的多个VLAN内发送ARP请求，由于trunk间允许的VLAN数量众多，实际使用的也达到约40个，所以在每个VLAN都发送ARP请求的情况下， S9508_1向S9508_2每秒发送的ARP请求数量会达到约40pps。而由于S9508_2开启了ARP防攻击功能，在S9508_2检查收到的这些ARP报文的时候，会发现它们的源MAC地址都相同，且发送频率超过了默认ARP防攻击门限值30pps，于是S9508_2认为发生了ARP攻击，打印信息进行告警。

四、 解决方法：

问题产生的根源是多个VLAN发送ARP请求，频率超过了ARP防攻击门限值，所以有两个方法解决此问题：

1.调整门限值，使得正常的ARP请求数量在该门限值以下，但由于该修改是全局性的，若网络中真的发生了ARP攻击，则会出现漏报的情况，因此我们不建议修改该值。

[H3C]anti-attack arp threshold 60

2.配置命令，将000f-e2a4-e36c 这个设备虚接口的MAC地址配置为安全mac，从防攻击侦测中剔除。

[H3C] anti-attack arp exclude-mac 000f-e2a4-e36c

我们建议采用该方式，并将所有重要设备的mac都列为安全mac，保证不会出现防攻击导致的重要设备断网或告警。