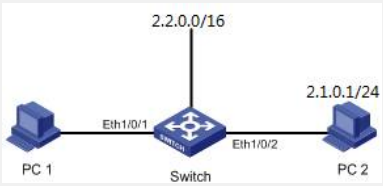
某局点S5800交换机开启ARP Detection后出现网络中断的异常问题

DHCP 郭智科 2012-08-09 发表

某局点S5800交换机开启ARP Detection后出现网络中断的异常问题

一、 组网:



二、 问题描述:

某局点使用H3C S5800交换机做DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）中继，为下联终端提供地址分配的服务，该交换机通过三层路由口和DHCP服务器相连。后期随着客户网络的扩容和对网络安全的更高要求，客户希望增强网络的安全性，于是想使用一定的安全策略保证接入用户的身份和安全。于是现场工程师小G充分的了解了用户需求后，结合现场的实际情况（下联终端使用DHCP协议自动获取IP地址），决定使用交换机ARP Detection和DHCP SNOOPING相结合的功能对用户合法性进行检查，以防止仿冒用户的攻击。于是他在S5800交换机上添加了如下配置:

dhcp-snooping

vlan 2

arp detection enable

当配置完成后发现，接入终端会在一段时间之后出现网络中断的情况，重启电脑终端后才能恢复，但是问题一直存在。于是小G有点困惑了，为什么会出现这种奇怪现象呢?

三、 过程分析:

既然开启了ARP Detection和DHCP SNOOPING功能后才出现了异常中断的现象，那么现场出现的这个问题肯定和这两个新功能有着很直接的关系。于是小G根据ARP Detection的功能原理分析判断是否安全表项没有正确建立或者一段时间后老化?

因此查看交换机DHCP Snooping安全表项发现，网络中断的时候确实没有安全表项。那么可以推断，这个正常时间段必定是DHCP服务器分配的IP地址的租期。因为这个租期就是DHCP Snooping安全表项的老化时间。重启电脑终端后恢复是因为重新创建了安全表项。display dhcp-snooping

DHCP Snooping is enabled.

The client binding table for all untrusted ports.

Type : D--Dynamic , S--Static , R--Recovering

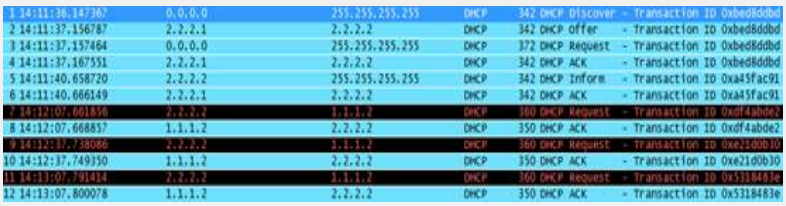
Type IP Address MAC Address Lease VLAN SVLAN Interface

==== ============== ============== ============ ==== ===== ==========

--- 0 dhcp-snooping item(s) found ---

既然DHCP服务器分配的IP地址的租期就是DHCP Snooping安全表项的老化时间，为什么下联终端的IP地址一直存在呢？既然IP地址一直存在，就证明IP地址有了续约的过程，租期已经刷新，那为什么DHCP Snooping安全表项的老化时间没有刷新呢?

小G抓包发现，下联终端在使用IP的过程中，终端发送的DHCP报文如下:



抓包中可以清楚看到，IP地址租期一直在续约。既然IP地址租期一直有刷新，为什么DHCP Snooping安全表项的老化时间没有刷新呢?

我们知道，DHCP Snooping安全机制允许将端口设置为信任端口和不信任端口。当设备开启DHCP Snooping特性后，会触发软件驱动下发如下几条表项:

udp dport 68//全局丢弃
udp dport 67//全局重定向上cpu
udp dport 68 dip 255.255.255.255 copy上cpu
注：udp dport 68是server端发送的报文，67是client端发送的报文。
使能DHCP Snooping功能后，只有相应端口配置了trust（设置为信任端口），才会触发对该端口下发一个dport 68上送cpu，同时驱动会把该端口从全局丢弃的表项中去掉，这样server发送的68的单播报文就可以上送给软件平台，这时候才能刷新DHCP Snooping表项。如果是不信任端口，报文无法上送软件平台，所以DHCP Snooping表项无法被刷新，这样就知道表项无法刷新的原因了。

四、 解决方法：

既然相应端口设置为信任端口，才能刷新DHCP Snooping表项。那么只需要将连接DHCP服务器端口设置为信任端口即可。但是由于5800交换机使用三层路由口和服务器相连，目前不支持三层口配置trust，所以就现场环境来说，只能使用三层虚接口方式代替三层路由口，将相应物理端口配置为信任端口来解决该问题。

特别说明：

一般情况下，不建议在同一台设备上开启DHCP Snooping和DHCP Relay功能。