Comware V7 平台交换机开启 arp ip-confict log prompt 功能后提示IP地址冲突经验案例

ARP攻击防御 ARP 丁犁 2021-08-31 发表

组网及说明

不涉及

问题描述

使用 S10500X 系列交换机（ R7596P05 版本）进行说明：该交换机设备作为用户终端的网关设备，在其上配置相应 Vlan-interface 虚接口，并开启ARP 防护功能。

```
#
 interface Vlan-interface2001
 ip address 20.20.101.254 255.255.255.0
#
 arp valid-check enable  //开启ARP报文源MAC地址一致性检查功能
 arp ip-conflict log prompt  //开启源IP地址冲突提示功能
 arp source-mac filter  //使能源MAC地址固定的ARP攻击检测功能
 arp source-mac threshold 25  //源MAC地址固定的ARP报文攻击检测的阈值为25
 arp source-suppression enable  //开启ARP源地址抑制功能
 arp source-suppression limit 8  //配置ARP源抑制的阈值为8 (在5秒间隔内可以处理的源IP相同，但目的IP地址不能解析的IP报文的最大数目为8)
#

Vlan-interface2001
Current state: UP
Line protocol state: UP
Description: Vlan-interface2001 Interface
Bandwidth: 10000000 kbps
Maximum transmission unit: 1500
Internet address: 20.20.101.254/24 (Primary)
IP packet frame type: Ethernet II, hardware address:74d6-cbc5-9401
IPv6 packet frame type: Ethernet II, hardware address: 74d6-cbc5-9401
.....
```

部署后，交换机上提示存在网关 20.20.101.254 地址冲突（网关的 MAC = 74d6-cbc5-9401，冲突的 MAC= c074-ad44-b542 ）：

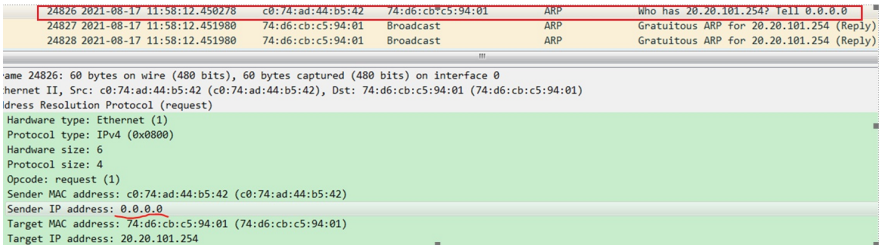
```
 %Aug 12 18:31:54:690 2021 PingShan_Neiwang_coreswitch ARP/6/DUPIFIP: -Chassis=1-Slot=7; Duplicate address 20.20.101.254 on interface Vlan-interface2001, sourced from c074-ad44-b542
```

过程分析

分析一：

观察提示冲突的 MAC 地址为 c074-ad44-b542 的终端，发现其为 IP 话机，缺省没有IP地址，需要从 DHCP Server 上获取 IP 地址。

通过抓取 IP 话机上线过程（获取 IP 地址过程），发现话机会向交换机网关（ MAC = 74d6-cbc5-9401 ），发送如下图所示的 特殊ARP报文：



IP 话机发送的此 ARP 报文，其中 Sender IP address 为空，即 0.0.0.0。

正常情况下，网络中不应该出现这种 Sender IP address = 0.0.0.0 的报文，但对于一些特殊的终端、话机、或部分版本的 Windows 系统开机后会发送类似的报文，作为免费ARP使用，使得终端能够判断网络中是否存在网关 IP 地址冲突的情况。

分析二：

由于交换机上，部署了开启源IP地址冲突提示功能，及设备接收到其它设备发送的ARP报文后，如果发现报文中的源IP地址和自己的IP地址相同，该设备会立刻提示存在IP地址冲突。

#

.....

arp ip-conflict log prompt //开启源IP地址冲突提示功能

.....

#

分析三：

对于 IP 话机发送的 Sender IP address 为空，0.0.0.0 的 ARP报文，当交换机接收到后，底层逻辑会认为该字段为空时，表示“any”匹配所有。

结合 分析一 和 分析二 ，可确认当交换机使能了“arp ip-conflict log prompt”功能后，当收到 Sender IP adress = 0.0.0.0 的 ARP 报文，与本地 Vlan-interface 2001 的网关 IP 地址相同时，就会出现提示网关 IP 地址冲突的日志。

解决方法

解决方法一：调整终端话机设置，使其不发送相关特殊的ARP报文（Sender IP address = 0.0.0.0，Target IP address = 网关 IP 地址）
解决方法二：将“arp ip-conflict log prompt”命令删除，避免设备打印提示冲突告警信息。