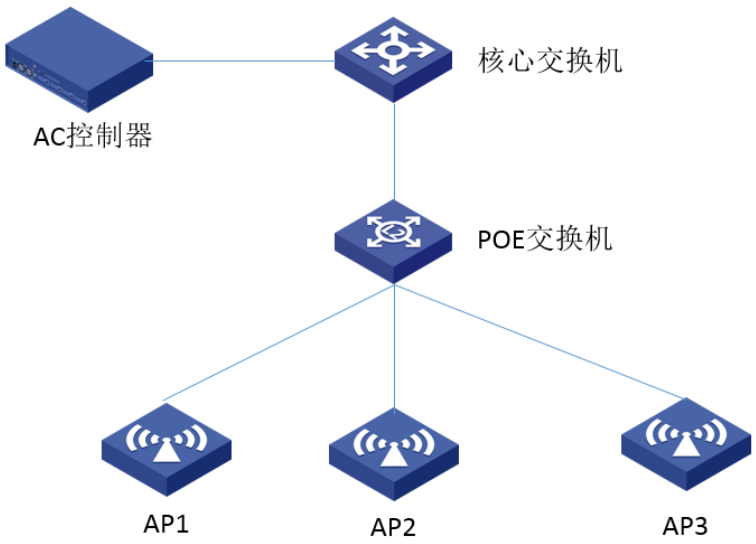
# 某局点ap本地转发模式下开启二层隔离仍然有部分终端能够互访（二层隔离部分不生效）

VLAN 柴鹏辉 2019-03-25 发表

## 组网及说明

1.组网

WX系列AC控制器，fit系列AP，交换机二层设备




2.问题描述

客户反馈采用本地转发的模式，AP为WA6528，开启了基于vlan的用户隔离，但是三个ap下的的终端部分间能够实现vlan内二层互访（如：AP1下的终端和AP3不能互访，但是可以和AP2下关联的终端能够互访），怀疑是二层隔离有问题。

现象截图：

（1）ap1和ap2下联终端不能互访（二层隔离生效）

```
C:\Users\MyPC>ping 10.186.145.168

正在 Ping 10.186.145.168 具有 32 字节的数据:
来自 10.186.145.139 的回复: 无法访问目标主机。
来自 10.186.145.139 的回复: 无法访问目标主机。
来自 10.186.145.139 的回复: 无法访问目标主机。
来自 10.186.145.139 的回复: 无法访问目标主机。

10.186.145.168 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
```

（2）ap1和ap3下的终端可以互访（二层隔离不生效）

```
C:\Users\MyPC>ping 10.186.93.54

正在 Ping 10.186.93.54 具有 32 字节的数据:
来自 10.186.93.54 的回复: 字节=32 时间=597ms TTL=62
来自 10.186.93.54 的回复: 字节=32 时间=598ms TTL=62
来自 10.186.93.54 的回复: 字节=32 时间=607ms TTL=62
来自 10.186.93.54 的回复: 字节=32 时间=276ms TTL=62

10.186.93.54 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 276ms, 最长 = 607ms, 平均 = 519ms
```

## 问题描述

3、问题分析过程

（1）查看ac侧基本配置：

```
wlan ap 1 model WA6528
 serial-id 219801A1LH818C000001
 description 1004
 map-configuration cfa0:/apcfg.txt
```

```
 vlan 1
 radio 1
  channel 149
  radio enable
  service-template 1 vlan 1600
 radio 2
  channel 1
  radio enable
  service-template 1 vlan 1600
 gigabitethernet 1
 gigabitethernet 2
 smartrate-ethernet 1
#
wlan ap 2 model WA6528
 serial-id 219801A1LH818C000002
 description 1004
 map-configuration cfa0:/apcfg.txt
 vlan 1
 radio 1
  channel 149
  radio enable
  service-template 1 vlan 1600
 radio 2
  channel 1
  radio enable
  service-template 1 vlan 1600
 gigabitethernet 1
 gigabitethernet 2
 smartrate-ethernet 1
#
wlan ap 3 model WA6528
 serial-id 219801A1LH818C000003
 description 1004
 map-configuration cfa0:/apcfg.txt
 vlan 1
 radio 1
  channel 149
  radio enable
  service-template 1 vlan 1600
 radio 2
  channel 1
  radio enable
  service-template 1 vlan 1600
 gigabitethernet 1
 gigabitethernet 2
 smartrate-ethernet 1
#
```

（2）查看ap诊断

ap1、ap2和ap3的基本诊断如下（三个相同，仅以一个为例）：

```
interface Vlan-interface1
 ip address dhcp-alloc
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 1600
 port-isolate enable
#
interface GigabitEthernet1/0/2
 port-isolate enable
#
interface WLAN-Radio1/0/1
#
interface WLAN-Radio1/0/2
#
```

```
interface Smartrate-Ethernet1/0/1
 port-isolate enable
#
 scheduler logfile size 16
#
line class console
#
line class vty
#
line con 0
#
line vty 0 4
 set authentication password hash
$h$6$SV/rLgzn9MHCHrLy$eAoKRrAZeCA97Y/pUKO57tot8WTZRJr6yHwMhWAAT7h7l6A4aALordkC
4O+YHXDeOZWH78aNdgS9dPgIU99GaQ==
#
line vty 5 63
#
 undo gratuitous-arp-learning enable
#
domain system
#
 domain default enable system
#
user-group system
#
 user-isolation vlan 1600 enable
 user-isolation vlan 1600 permit-mac 8800-f3b2-51ef
#
return
```

## 过程分析

无线网络中的二层隔离分为两种：

（1）基于ssid的用户隔离使得终端之间无法互访，但是对网关不做限制。

（2）基于vlan的二层隔离，是在该vlan内终端用户不能实现二层互访，但是可以通过放通命令：**user-isolation vlan ** permit-mac ********** 实现用户的二层互访，这种情况下通常也需要放通网关地址。从ap的诊断信息来看，vlan内的用户隔离配置已经下发到ap上，因此本应当生效。但是，出现部分用户可以互访。因此需要进一步考虑哪些部分可能会导致该问题，我们可以看到基于vlan的用户隔离是放通网关的mac地址的，因此就有存在可以互访的终端能够ping通，是否是通过网关访问的（源地址已经更改为了网关地址），由于网关为华为交换机，没办法查看华为交换机的配置，只能通过抓包验证猜想：指导客户抓取可以互访的空口报文，通过查看，果然源地址更改为网关地址，因此二层隔离不生效。进一步和代理商确认，代理商反馈核心交换机上开启了arp代理功能，可能是该问题导致。建议客户删除该配置进行验证，发现的确为这个原因，至此，问题已经得到定位。

## 解决方法

指导客户删除网关设备上的arp代理功能，二层隔离生效。