二层隔离场景下本地转发AC与终端偶发20分钟不通

wlan接入 AP管理 **聂冬** 2022-12-01 发表

组网及说明

AC——SW——AP

本地转发

AP上开启二层隔离

问题描述

二层隔离场景下本地转发AC与终端偶发20分钟不通

AC与终端为三层，AC上又起了与终端同网段的IP地址

终端每上线前十几分钟，与AC无法ping通。

十几分钟后，能正常ping通

过程分析

1、在故障的十几分钟期间，通过在AC到终端沿途流统抓包，发现AC回复了icmp response，在AP上行接入交换机也做了流统，icmp response都是正常转发的，但是在AP上收集debug信息，发现只有终端发的icmp request请求，没有回复。

AC icmp debug：有回复

*Sep 29 18:17:48:087 2022 AC NWT-WIFI-AC-WX5540X-1 SOCKET/7/ICMP:
ICMP Input:
ICMP Packet: src = 10.88.163.200, dst = 10.88.163.90
type = 8, code = 0 (echo)
*Sep 29 18:17:48:087 2022 AC NWT-WIFI-AC-WX5540X-1 SOCKET/7/ICMP:
ICMP Output:
ICMP Packet: src = 10.88.163.90, dst = 10.88.163.200
type = 0, code = 0 (echo-reply)

而在AP上debug，只有终端发出的icmp，没有AC回复的icmp

后通过观察AC学习的终端ARP信息，对应的mac为终端的实际mac：

对ac侧来说，终端上线发的arp请求或者免费arp，ac能收到，因为二层隔离，无线到有线的广播不隔离。所以ac的arp表有终端而且是终端自己的地址

而终端上学习的AC ARP，学习到的为网关代答的，所以对应mac为网关mac：

Ping丢包过程：

AC 发送的icmp 源mac：自己 目的mac：终端

由于AP上开启二层隔离，未放通AC的mac，所以AC发送的报文被丢掉，进而不通。

20分钟AC自己学习到的终端arp老化后，重新学习到的终端arp为网关代答，通信回复正常。

解决方法

删除AC上的二层地址，通过三层转发进行通信。