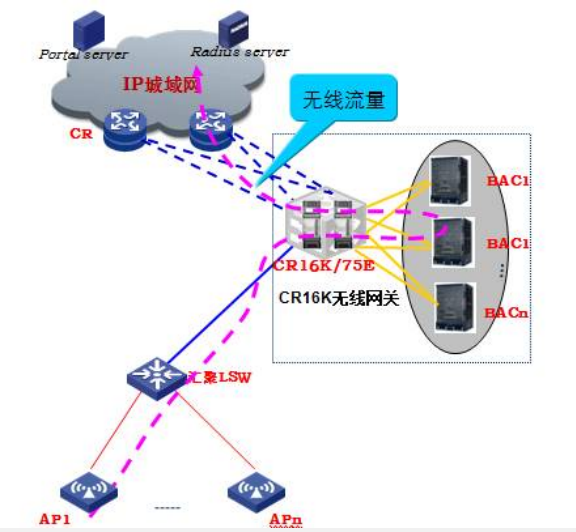
无线Portal认证支持通过dhcp-snooping获取用户信息的应用案例

Portal DHCP 李晨光 2013-10-25 发表

无线Portal认证支持通过dhcp-snooping获取用户信息的应用案例

一、组网架构：

在普通的三层Portal中，AC作为无线用户的网关，在三层VLAN接口上起Portal认证。但在某些特定的应用组网中，AC需要做二层转发，无线用户的业务网关在上联核心交换机上。本案例描述的是AC在这种二层转发的环境下做Portal认证的典型案例。



如上图，某运营商AC旁挂核心CR16K，AC做二层业务转发，业务网关在CR16K，用户地址池由CR16K分配。AC对无线用户做Portal认证。

二、问题描述：

在这种二层Portal组网环境下，有用户概率性出现Portal认证不通过的问题。排查原因定位为AC设备缺少用户的ARP表项，导致Portal Challenge挑战失败，认证拒绝。

特别的，当在某些特殊的应用场景下，如AC池场景下，为减少IP地址的浪费和简化运维，AC Portal认证三层接口可以不配置IP地址。在这种情况下AC就根本无法学习用户的ARP了，Portal用户检查也会通不过，Portal认证失败。

三、问题分析和解决方案：

无线AC收到Portal服务器针对某个IP用户的认证请求后，需要先确认该IP地址的无线用户确实存在于AC上，即确认IP和用户MAC的对应关系。确认的方法有ARP或者DHCP-SNOOPING。但在二层Portal环境下，AC仅做二层转发，会某些终端原因导致学不到ARP。而且关键的是当AC上的Portal接口没有配置IP地址时，AC根本没法学习用户的ARP，最终导致Portal认证失败。

解决办法是让AC通过DHCP-SNOOPING方式获取用户信息。DHCP-SNOOPING即DHCP服务的二层监听功能，开启DHCP-SNOOPING功能后，设备就可以从接收到DHCP-ACK和DHCP-REQUEST报文中提取并记录IP地址和MAC地址信息。在该案例组网中，AC做二层转发，无线用户通过DHCP从上联CR16K获取IP地址。AC开启了DHCP-SNOOPING后即可以获取用户IP和MAC对应关系，完成Portal认证。

配置命令：配置Portal用户信息获取的方式为DHCP-SNOOPING

```
[H3C] portal host-check dhcp-snooping
```

注意事项：全局需要先开启dhcp-snooping并放通AC内联口。