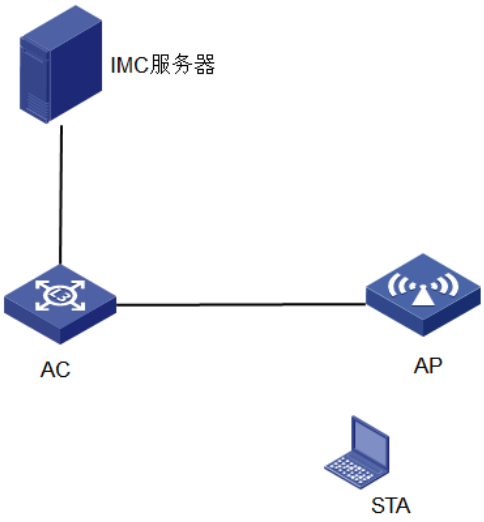
基于AP的无线终端准入典型配置（V7）

裴锐霖 2018-03-25 发表

有些局点需控制终端的接入范围，比如终端A只能接入AP1和AP2，终端B只能接入AP3和AP4，但SSID只有一个，这种情况下可以通过MAC认证结合下发user-profile来实现基于AP的终端准入。如果有Radius服务器，则通过Radius服务器可以下发，如果没有Radius服务器，通过本地MAC认证在V7上也可以下发。



方案1、结合IMC做MAC认证，要求用户1只能关联宿舍区的AP1和AP2，用户2只能关联教室区的AP3和AP4。

#创建radius方案名称为mac

[AC-radius-mac]primary authentication 172.31.3.252 key simple h3c

[AC-radius-mac]primary accounting 172.31.3.252 key simple h3c

创建一个名称为mac的认证域

[AC] domain local-mac

[AC-isp-local-mac]authentication lan-access radius-scheme mac

[AC-isp-local-mac]authorization lan-access radius-scheme mac

[AC-isp-local-mac]accounting lan-access radius-scheme mac

[AC] wlan service-template 1

配置SSID为service。

[AC-wlan-st-1] ssid service

配置客户端从无线服务模板1上线后会被加入VLAN 200。

[AC-wlan-st-1] vlan 200

配置客户端接入认证方式为MAC地址认证。

[AC-wlan-st-1] client-security authentication-mode mac

配置MAC地址认证用户使用的ISP域为local-mac。

[AC-wlan-st-1] mac-authentication domain mac

开启无线服务模板。

[AC-wlan-st-1] service-template enable

#创建AP组，一个为sushe，一个为jiaoshi

[AC]wlan ap-group sushe

[AC-wlan-ap-group-sushe]ap ap1 ap2

[AC]wlan ap-group jiaoshi

[AC-wlan-ap-group-sushe]ap ap3 ap4

#创建user-profile user1 和user2

[AC]user-profile user1

[AC-user-profile-mac]wlan permit-ap-group sushe

[AC]user-profile user2

[AC-user-profile-mac]wlan permit-ap-group jiaoshi

方案2、本地MAC认证下发User-profile，基于上面的配置将远程Dot1x改成本地Dot1x认证即可。

local-user a80c63dc2423 class network

password simple a80c63dc2423

service-type lan-access

authorization-attribute user-profile sushe

authorization-attribute user-role network-operator

关键点：User-profile基于AP组控制终端的接入，所以AC上只需要创建相应名字的User-profile即可，Radius认证下发后会自动调用。

#创建user-profile user1 和user2

[AC]user-profile user1

[AC-user-profile-mac]wlan permit-ap-group sushe

[AC]user-profile user2

[AC-user-profile-mac]wlan permit-ap-group jiaoshi