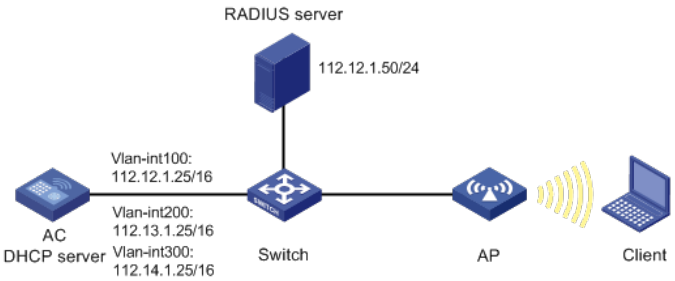
Mac or Portal无感知认证配置典型案例

MAC地址认证 Portal 杨攀 2017-05-10 发表

WX系列AC、FIT AP、便携机（安装有无线网卡）、Radius/Portal Server技术原理介绍：中国移动主推的Portal无感知认证是基于流量触发mac-triger，要求支持移动的mac-triger协议，并且新增MAC绑定服务器以存储MAC的绑定关系。对于第三方的Radius/Portal server厂商来说开发较繁琐，有些厂商是不支持的。如果不支持mac-triger协议，可以采用MAC bypass portal的认证方式。
具体实现流程如下所示：
（1）仍然借助guest-vlan，但guest-vlan跟业务VLAN是相同的。也就是说相同VLAN中MAC认证和Portal认证二选一即可，不存在VLAN切换的事情了；
（2）用户首次上线，MAC认证失败会弹出portal页面，进行portal认证。portal认证通过后可以直接上网；
（3）用户再次上线，如果对应portal用户存在，不会发起MAC认证，可以直接上网；
（4）用户再次上线，如果对应portal用户不存在，则发起MAC认证。MAC认证成功后不会再弹出Portal页面，可以直接上网；
（5）display connection中只会看到一个连接，Portal的或者MAC认证的；
备注：该方案中，第三方Radius/Portal server除需具有Radius服务器和Portal服务器的功能外，关键的需要有通过Portal认证过程得到用户的MAC地址，并将该MAC地址创建为合法的MAC用户名的功能。

组网信息及描述
如图1所示，集中式转发架构下，AP和Client通过DHCP server获取IP地址，设备管理员希望实现无感知，当第一次进行了portal认证成功之后，后面就无感知进行上线，具体要求如下：
配置VLAN 200为Client的接入VLAN，当Client的MAC地址认证失败时进入Guest VLAN，进入guest vlan之后就触发portal认证。



一、 配置AC
(1) 配置AC的接口
创建VLAN 100及其对应的VLAN接口，并为该接口配置IP地址。AP将获取该IP地址与AC建立CAPWAP隧道。
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 112.12.1.25 16
[AC-Vlan-interface100] quit
创建VLAN 200及其对应的VLAN接口，并为该接口配置IP地址。Client使用该VLAN接入无线网络。
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 112.13.1.25 16
[AC-Vlan-interface200] quit
配置AC和Switch相连的接口GigabitEthernet1/0/1为Trunk类型，禁止VLAN 1报文通过，允许VLAN 100、VLAN 200通过，当前Trunk口的PVID为100。
[AC] interface gigabitEthernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
(2)配置DHCP server
开启DHCP server功能。
[AC] dhcp enable

配置DHCP地址池vlan100，为AP分配的地址范围为112.12.0.0/16，网关地址为112.12.1.25。
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 112.12.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan100] gateway-list 112.12.1.25
[AC-dhcp-pool-vlan100] quit
配置DHCP地址池vlan200，为Client分配的地址范围为112.13.0.0/16，网关地址为112.12.1.25。
[AC] dhcp server ip-pool vlan200
[AC-dhcp-pool-vlan200] network 112.13.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan200] gateway-list 112.12.1.25
[AC-dhcp-pool-vlan200] quit
(3)配置RADIUS认证
创建名为office的RADIUS方案，并进入其视图。
[AC] radius scheme office
配置主认证、计费RADIUS服务器的IP地址为112.12.1.50。
[AC-radius-office] primary authentication 112.12.1.50
[AC-radius-office] primary accounting 112.12.1.50
配置RADIUS认证、计费报文的共享密钥为123456789。
[AC-radius-office] key authentication simple 123456789
[AC-radius-office] key accounting simple 123456789
配置发送给RADIUS服务器的用户名不携带域名。
[AC-radius-office] user-name-format without-domain
配置设备发送RADIUS报文使用的源IP地址为112.12.1.25。
[AC-radius-office] nas-ip 112.12.1.25
[AC-radius-office] quit
创建名为office1的ISP域，并进入其视图。
[AC] domain office1
为lan-access用户和portal用户配置认证、授权、计费方案为RADIUS方案office。
[AC-isp-office1] authentication lan-access radius-scheme office
[AC-isp-office1] authorization lan-access radius-scheme office
[AC-isp-office1] accounting lan-access radius-scheme office
[AC-isp-office1] authentication portal radius-scheme office
[AC-isp-office1] authorization portal radius-scheme office
[AC-isp-office1] accounting portal radius-scheme office
配置用户闲置切断时间为15分钟，闲置切断时间内产生的流量为1024字节。
[AC-isp-office1] idle-cut enable 15 1024
[AC-isp-office1] quit
配置MAC地址认证的用户名和密码均为用户的MAC地址，且不带连字符（该配置为缺省配置）。
[AC] mac-authentication user-name-format mac-address without-hyphen lowercase
(4)配置WLAN-ESS接口
创建WLAN-ESS接口1，并进入接口视图。
[AC] interface wlan-ess 1
配置客户端获取的VLAN 为200。
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] mac-vlan enable
配置客户端接入认证方式为MAC地址认证。
[AC-WLAN-ESS1] port-security port-mode mac-authentication
配置MAC地址认证用户使用的ISP域为office1。
[AC-WLAN-ESS1] mac-authentication domain office1
配置MAC认证失败后的guest vlan
[AC-WLAN-ESS1] mac-authentication guest-vlan 200
#配置bypass portal的认证方式
[AC-WLAN-ESS1] mac-authentication bypass-portal enable
(5)配置portal认证
配置Portal服务器地址为112.12.1.50，并指定服务器对应的url。
[AC] portal server imc ip 112.12.1.50 key simple h3c url http:// 112.12.1.50:8080/portal
配置Portal免认证规则1，用于放行AC上起portal的接口能够与portal服务器通信。
[AC] portal free-rule 1 source interface bridge-aggregation1 destination any
[AC] interface vlan-interface 200
配置接口VLAN 200为Portal直接认证的接口。
[AC-Vlan-interface200] portal server imc method direct
指定从接口接入的IPv4 Portal用户使用认证域为office1。

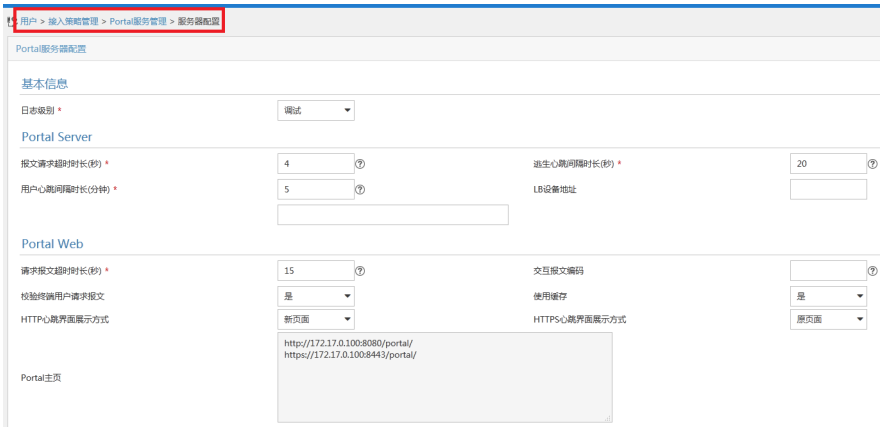
[AC-Vlan-interface200] portal domain office1
配置接口发送Portal报文使用的IPv4源地址为112.12.1.25。
[AC-Vlan-interface200] portal nas-ip 112.12.1.25
[AC-Vlan-interface200] quit
（6）配置服务模板
[AC] wlan service-template 1 clear
绑定wlan-ess接口。
[AC-wlan-st-1] bind WLAN-ESS 1
配置SSID为test。
[AC-wlan-st-1] ssid test
开启无线服务模板。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
(7)配置射频接口并绑定服务模板
创建手工AP，名称为officeap，型号名称为WA4320i-ACN。
[AC] wlan ap officeap model WA4320i-ACN
设置AP序列号为210235A1Q2C159000020。
[AC-wlan-ap-officeap] serial-id 210235A1Q2C159000020
进入AP的Radio 2视图，并将无线服务模板1绑定到Radio 2上。
[AC-wlan-ap-officeap] radio 2
[AC-wlan-ap-officeap-radio-2] service-template 1
开启Radio 2的射频功能。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit

二、配置Switch

创建VLAN 100、VLAN 200，其中VLAN 100用于转发AC和AP间CAPWAP隧道内的流量，VLAN 200用于转发Client无线报文，VLAN 300用于转发Guest VLAN的报文。
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
配置Switch与AC相连的GigabitEthernet1/0/1接口的属性为Trunk，禁止VLAN 1报文通过，允许VLAN 100通过，当前Trunk口的PVID为100。
[Switch] interface gigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
配置Switch与AP相连的GigabitEthernet1/0/2接口属性为Access，并允许VLAN 100通过。
[Switch] interface gigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
开启PoE接口远程供电功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit

三、配置RADIUS服务器

下面以iMC为例（使用iMC版本为：iMC PLAT 7.1(E0303P10)、iMC UAM 7.1(E0303P10)，说明RADIUS server的基本配置。
登录进入iMC管理平台，选择“用户”页签，单击导航树中的[接入策略管理/Portal服务管理/服务器配置]菜单项，进入服务器配置页面，使用缺省配置。



配置IP地址组。

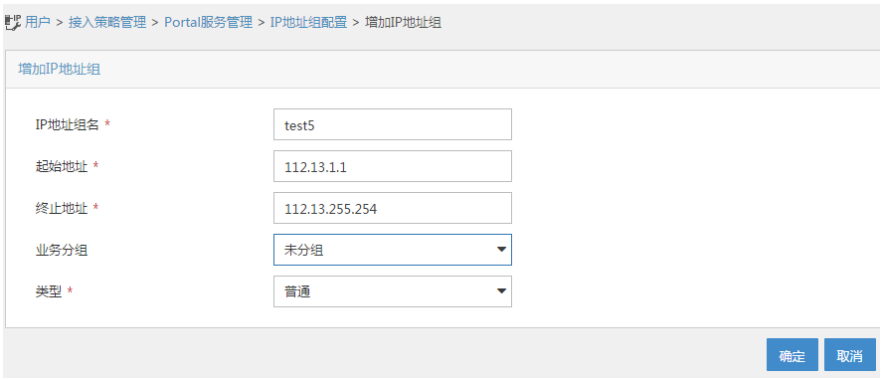
选择“用户”页签，单击导航树[接入策略管理/Portal服务管理/ IP地址组配置]菜单项，进入IP地址组配置页面，在该页面中单击<增加>按钮，进入增加IP地址组配置页面。

· 输入IP地址组名：test5；

·输入起始地址：112.13.1.1；

·输入终止地址：112.13.255.254；

其他采用缺省配置，单击<确定>按钮完成操作



增加Portal设备。

选择“用户”页签，单击导航树中的[接入策略管理/Portal服务管理/设备配置]菜单项，进入设备配置页面。在该页面中单击<增加>按钮，进入增加设备信息配置页面。

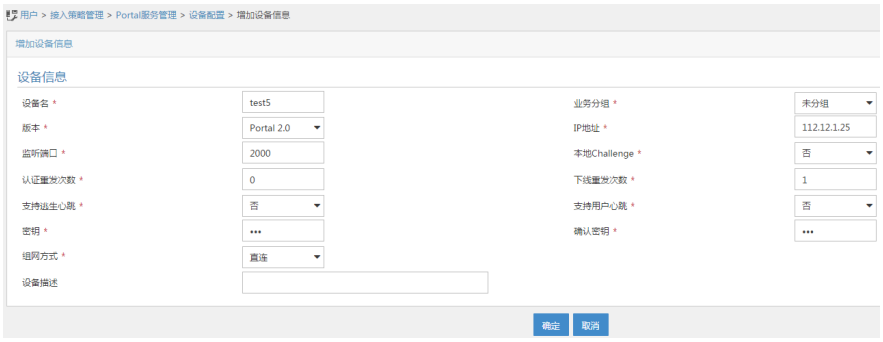
·输入设备名：test5；

·输入IP地址：即AC上配置的portal bas-ip地址，112.12.1.25；

·输入密钥：h3c，与AC上配置的portal server密钥一致；

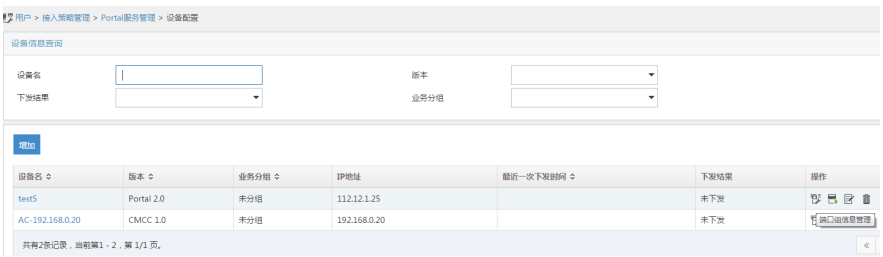
· 组网方式改为“直连”类型；

?其他采用默认配置，单击<确定>按钮完成操作。



增加端口组信息。

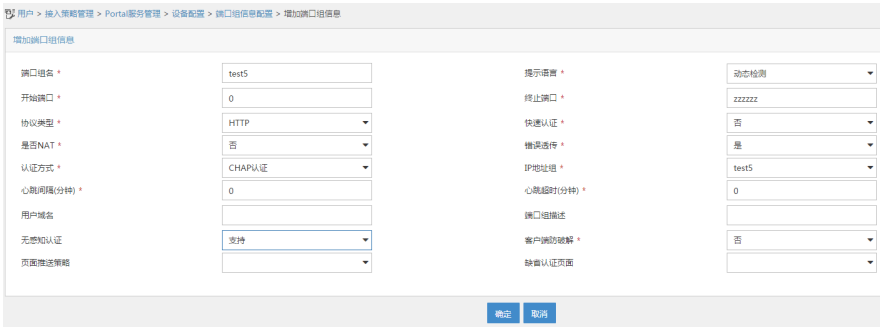
在Portal设备配置页面中的设备信息列表中，单击“ ”图标，进入端口组信息配置页面。



在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

· 输入端口组名：test5；

·选择IP地址组：test5；
· 选择支持无感知认证；
·其他采用默认配置，单击<确定>按钮完成操作。



配置接入服务

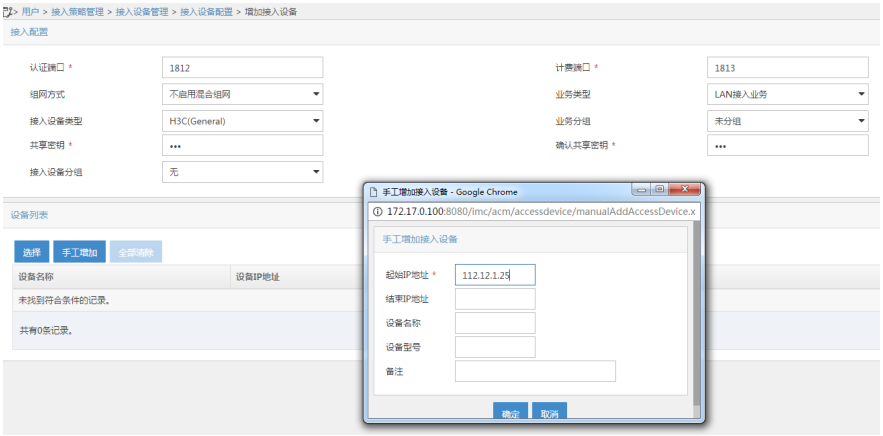
选择“用户”标签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面。在该页面中单击<增加>按钮，进入增加接入设备页面。

1、设置与AC交互报文时使用的认证、计费共享密钥为“h3c”，该密码与AC配置RADIUS方案时的地址一致；

2、选择接入设备类型为“H3C(General)”；

3、其它参数采用缺省值，并单击<确定>按钮完成操作

点击“选择”按钮；



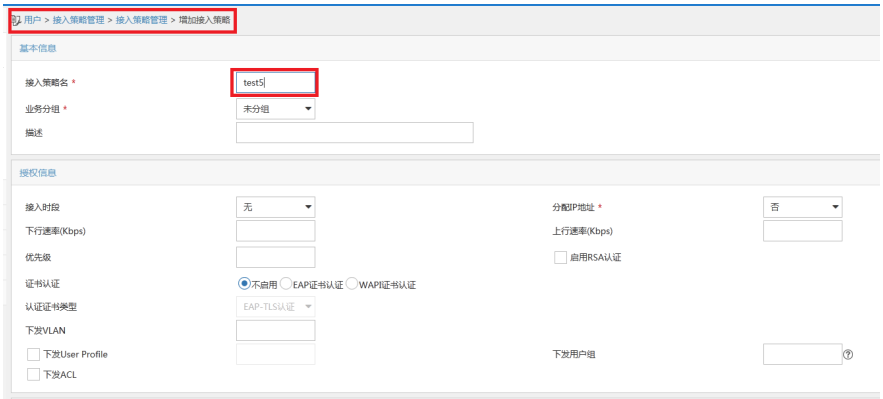
增加接入策略。

选择“用户”标签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略配置页面。在接入策略列表中点击<增加>按钮，进入增加接入策略页面。

· 接入策略名输入“test5”；

·业务分组“未分组”；

其它参数采用缺省值，并单击<确定>按钮完成操作



增加接入服务。

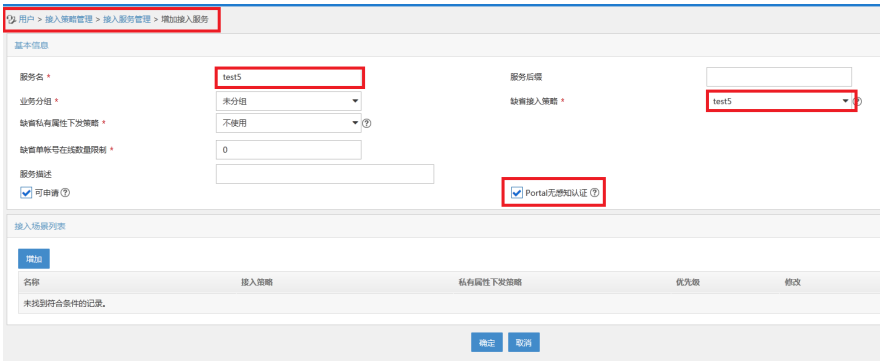
选择“用户”标签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入接入服务配置页面。在接入服务列表中点击<增加>按钮。

·服务名输入“test5”；

·缺省接入策略“test5”；

· 勾选portal无感知认证；

其它参数采用缺省值，并单击<确定>按钮完成操作。



增加接入用户。

选择“用户”标签，单击导航树中的[接入用户管理/接入用户]菜单项，进入到接入用户配置页面。在接入用户列表中点击<增加>按钮，进入增加接入用户页面。

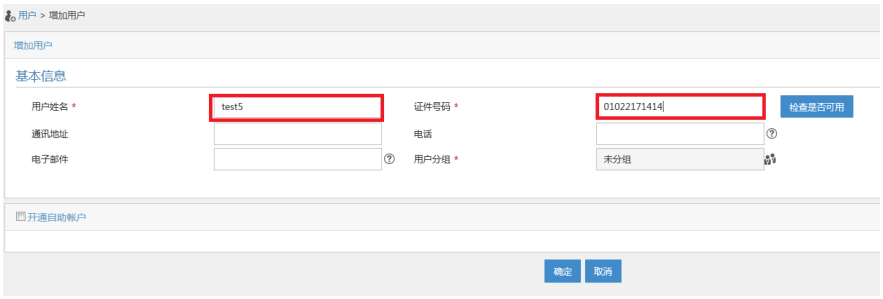
·在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；

·输入用户名“test5”；

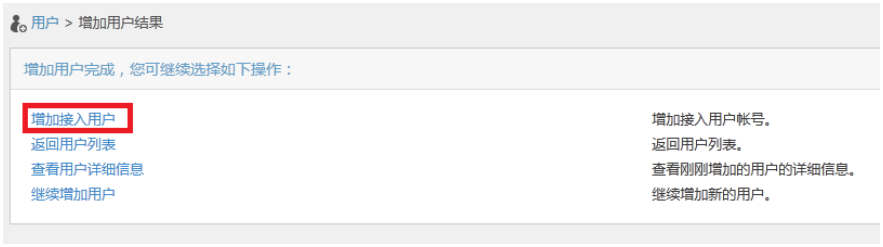
· 输入证件号码“01022171414”；

·单击<检查是否可用>按钮；

·如用户姓名和证件号码可用，单击<确定>按钮完成操作。



点击“确定”按钮，选择“增加接入用户”。



·账号名输入“test5”；

·密码输入“test5”；

·强portal无感知认证最大数设置为10；

·勾选接入服务

单击<确定>按钮完成操作。

五、验证配置

(1)用户使用智能终端通过浏览器访问网络，重定向到Portal认证页面。用户输入用户名、密码、服务等认证信息，进行上线认证。

(2)认证成功后，用户下线。

(3)用户再次使用该智能终端访问网络，这时不需要输入用户名和密码，直接上线。

(4)此时可在iMC上观察到绑定该智能终端MAC地址信息

AC上可以通过display connection 来进行查看

配置注意事项：

1、闲置时长idle-cut的命令一定要配置，强烈建议配置的闲置时长的时间少于客户端获取地址的租约时间的一半。

2、AC上虽然没有配置mac-trigger类型的无感知，但IMC上一定要勾选无感知。