# WX5002与iMC配合实现Portal EAD认证功能的典型配置

冯斯毅 2008-12-25 发表

**WX5002与iMC配合实现Portal EAD认证功能的典型配置**

适用WX5002版本：Comware Software, Version 5.20, Release 1106P01

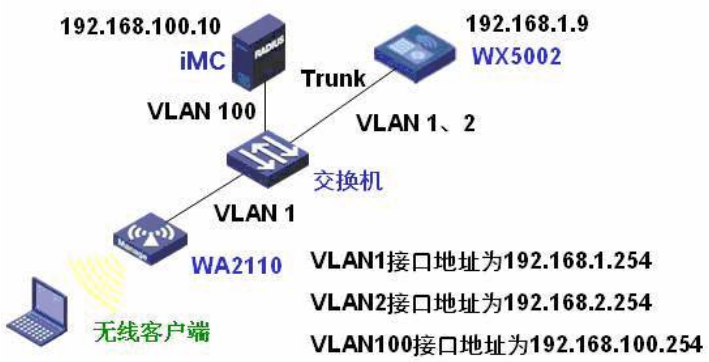
适用iMC UAM版本：V3.60-E6102

适用iNode版本：V2.40-R0319以上版本，要求支持Portal认证

**一、组网需求**

WX5002、WA2110、H3C POE交换机、便携机（安装有11b/g无线网卡）、iMC服务器

**二、组网图**




WX5002的IP地址为192.168.1.9。

交换机为三层交换机，交换机上VLAN1、2、100的接口地址分别是192.168.1.254、192.168.2.254和192.168.100.254。

WA2110在VLAN 1，WX5002和交换机之间为Trunk，通过VLAN1、2。

无线客户端属于VLAN 2，网关在交换机上为192.168.2.254。

iMC服务器在VLAN100，地址为192.168.100.10。

本例中WA2110的序列号为210235A22W0077000088。

SSID的名称为***wlan-ead***。

**三、WX交换机的典型配置**

```
#
 version 5.20, Release 1106P01
#
 sysname H3C
#
 domain default enable isp
#
 portal server newp ip 192.168.100.10 key portal url http://192.168.100.10
 portal free-rule 0 source any destination ip 192.168.2.0 mask 255.255.255.0
#
vlan 1
#
vlan 2
#
radius scheme radius1
 server-type extended
 primary authentication 192.168.100.10
 primary accounting 192.168.100.10
 key authentication h3c
 key accounting h3c
 user-name-format without-domain
 nas-ip 192.168.1.9
#
domain isp
 authentication portal radius-scheme radius1
 authorization portal radius-scheme radius1
 accounting portal radius-scheme radius1
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
```

```
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
dhcp server ip-pool 1
 network 192.168.1.0 mask 255.255.255.0
 gateway-list 192.168.1.254
 expired day 3
#
dhcp server ip-pool 2
 network 192.168.2.0 mask 255.255.255.0
 gateway-list 192.168.2.254
 expired day 3
#
wlan rrm
 dot11a mandatory-rate 6 12 24
 dot11a supported-rate 9 18 36 48 54
 dot11b mandatory-rate 1 2
 dot11b supported-rate 5.5 11
 dot11g mandatory-rate 1 2 5.5 11
 dot11g supported-rate 6 9 12 18 24 36 48 54
#
wlan service-template 2 clear
 ssid wlan-ead
 bind WLAN-ESS 2
 authentication-method open-system
 service-template enable
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.1.9 255.255.255.0
#
interface Vlan-interface2
 ip address 192.168.2.9 255.255.255.0
 portal server newp method direct
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan all
#
interface M-Ethernet1/0/1
#
interface WLAN-ESS2
 port access vlan 2
#
wlan ap ap1 model WA2100
 serial-id 210235A22W0077000088
 radio 1
  service-template 2
  radio enable
#
 ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
#
 dhcp enable
#
user-interface aux 0
user-interface vty 0 4
```

#
return

**四、iMC配置**

**1、配置Portal Server.**

**步骤1、配置设备信息**

配置设备信息，主要有:

IP地址：Station连接的WX5002上Wlan-ESS口所属vlan的三层口IP地址。本例中为192.168.2.9。

版本：portal 2.0

密钥：WX5002上配置的portal server 的密钥。本例中为“portal”。

注意：


**步骤2、增加IP地址组**

增加的ip地址组是指Station接入后获得的IP地址所属的网段，本例中Station获得的IP地址是192.168.2.0/24, 所以这里添加的ip地址组就是从192.168.2.1 到192.168.2.254。


**步骤3、配置端口管理信息**

主要配置端口组名和IP地址组，IP地址组选择步骤1中增加的IP地址组名。


**步骤4、配置生效**

配置完毕后，点击配置生效。

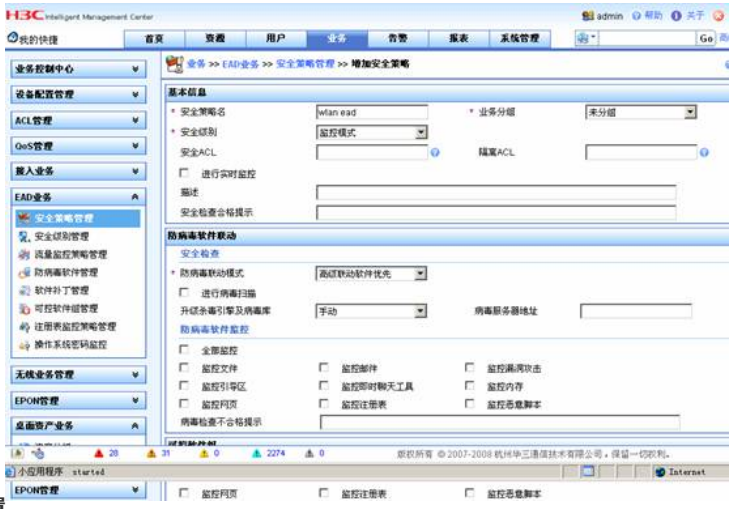

**2、接入设备配置**

在接入设备配置中将接入设备的IP地址加入。

保证设备的管理IP 192.168.1.9在添加的接入设备地址范围内192.168.1.1-192.168.1.254。

保证添加的接入设备的共享密钥与设备的配置一致，本例中为“h3c”


配置完毕后，点击配置生效。



**3、安全策略配置**

**4、服务配置**

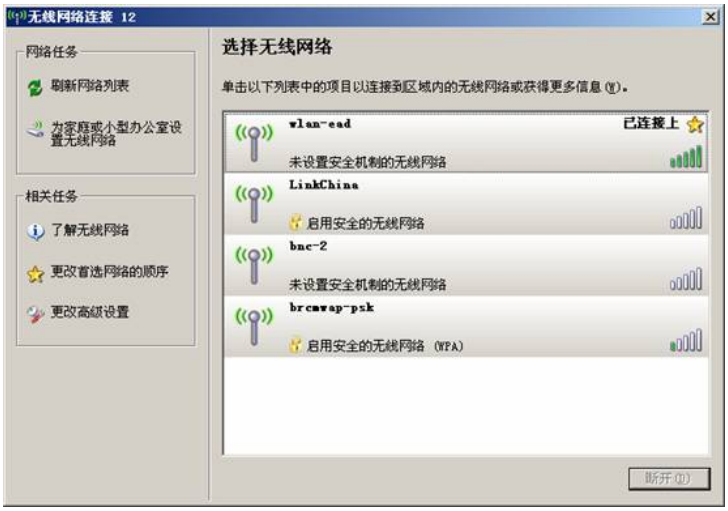
**5、用户帐户配置**

先增加平台用户

然后增加接入帐号

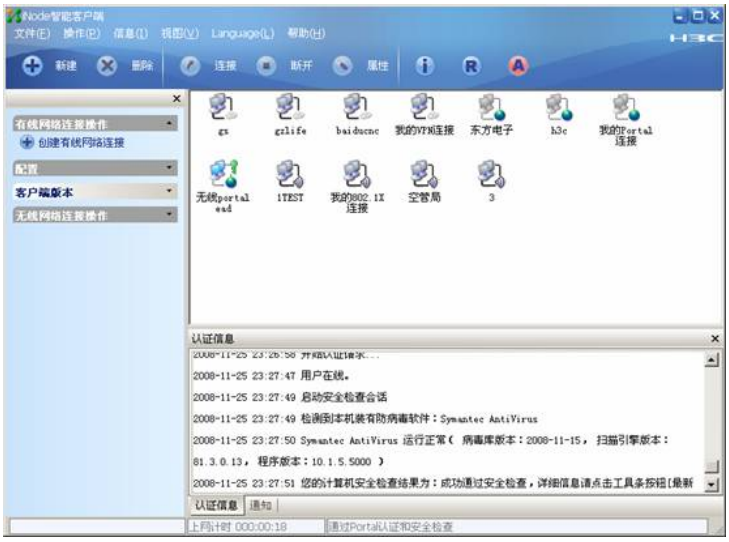

**6、验证结果**

**步骤1、连接SSID“H3C-Portal”，自动获取192.168.2.0/24网段地址。**





**步骤2、通过iNode发起认证，身份认证后会自动检查客户端安全状态。**




**7、FAQ**

1、默认情况下，Portal可以让广播报文和组播报文通过，所以未通过认证前Station也可以通过DHCP Server获得IP地址。

2、在未通过认证前，Station上线后应可以Ping通portal server.

3、需要添加开放整个客户端网段的Portal Free规则:

[wx5002] portal free 0 source ip any destination ip 192.168.2.0 mask 24

本例中要添加开放目的地址为客户端网段192.168.2.0/24的Portal Free rule。

4、如果通过DNS Server获取IP地址后上网，还需增加一条Portal Free规则:

[wx5002] portal free 1 source any destination ip 202.1.1.1 mask 32

202.1.1.1为DNS Server的IP地址。

5、AP和Station要在不同的网段，因为如果AP和Station在同一网段，在此网段启用Portal认证后会影响AP的注册。

6、AC radius scheme中一定要配置server-type extended。