WA2100和WX5002做无线接入并配合MA5200和Cams做Portal方式的EAD认证

张利兵 2007-07-04 发表

WA2100和WX5002做无线接入并配合MA5200和Cams做Portal方式的EAD认证

适用WA2100版本： Software Version V100R001B38D001

适用WX5002E版本：Software Version V100R001B38D001

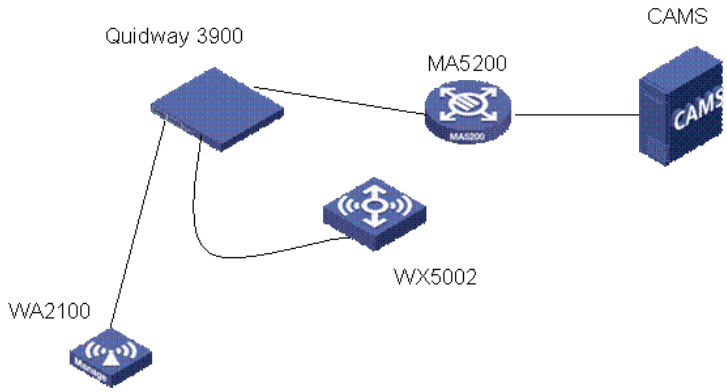
适用MA5200F版本：Version 2.10 RELEASE 7149 (SIMPLE)

适用CAMS版本：2.10-R0121 P03

一、 组网需求

WA2110、WX5002、交换机、MA5200F、CAMS服务器、便携机（安装有11b/g无线网卡和Windows无线客户端）

二、 组网图



无线客户端设置为自动获取IP地址方式

CAMS服务器的IP地址为192.168.0.100，网关为192.168.0.2

MA5200F的interface Ethernet19与CAMS连接，接口地址为192.168.0.2

MA5200F的interface Ethernet20与二层交换机连接

MA5200F中采用本地IP地址池为客户端分配地址

WA2110的IP地址为192.168.1.50

SSID的名称为*TEST*

三、 WX5002的配置

1) **配置无线接口**

[H3C]int WLAN-ESS 3

[H3C-WLAN-ESS3]

2) **配置服务模板**

[H3C]wlan service-template 3 clear

[H3C-wlan-st-3]ssid test

[H3C-wlan-st-3]bind WLAN-ESS 3

[H3C-wlan-st-3] authentication-method open-system

[H3C-wlan-st-3]service-template enable

3) **配置AP1**

[H3C] wlan ap ap1 model WA2100

[H3C-wlan-ap-ap1] serial-id H3CWA2100CD0930

4) **配置AP射频**

[H3C-wlan-ap-ap1] radio 1 type 11g

[H3C-wlan-ap-ap1-radio-1] max-power 10

[H3C-wlan-ap-ap1-radio-1] service-template 1

5) **使能所有射频**

[H3C] wlan radio enable all

WX5002的完整配置：

```
version 5.00, 0001

 sysname
H3C

igmp-snooping
vlan 1
 igmp-snooping enable
```

```
 igmp-snooping querier
 igmp-snooping general-query source-ip 192.168.0.100
#
vlan 2
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
local-user zlb

wlan service-template 3 clear
 ssid test
 bind WLAN-ESS 3
 authentication-method open-system
 service-template enable

wlan rrm
 11a mandatory-rate 6 12 24
 11a supported-rate 9 18 36 48 54
 11b mandatory-rate 1 2
 11b supported-rate 5.5 11
 11g mandatory-rate 1 2 5.5 11
 11g supported-rate 6 9 12 18 24 36 48 54
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.0.98 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
interface
GigabitEthernet1/0/2
interface M-
Ethernet1/0/1
interface WLAN-ESS3

wlan ap ap1 model WA2100
 serial-id H3CWA2100CD0930
 radio 1 type 11g
 max-power 10
 service-template 3
 radio enable

 snmp-agent
 snmp-agent local-engineid 000063A27F00000100007FDB
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 192.168.0.100 params securityname public

 load xml-configuration
#
user-interface aux 0
user-interface vty 0 4
#
dis wlan ap all ver
 Total Number of APs configured: 1
 Total Number of APs connected : 1
                    AP Profile: ap1
--------------------------------------------------------------------------------
 APID                    : 1
```

```
AP Name                      : ap1
State                        : Run
Up Time(hh:mm:ss)            : 00:01:33

Model                        : WA2100
Serial-ID                    : H3CWA2100CD0930
IP Address                   : 192.168.1.50

H/W Version                  : Ver.B
S/W Version                  : V100R001B38D001
Boot-Rom Version             : 107
Description                  : -NA-


Echo Interval(s)             : 10
Statistics report Interval(s) : 600

Cir(Kbps)                    : -NA-
Cbs(Bytes)                   : -NA-

Jumboframe Threshold         : Disable

Configuration Failure Count  : -NA-
Last Failure Reason          : -NA-

Last Reboot Reason           : Tunnel Initiated
--------------------------------------------------------------------------------
AP Mode                      : Split
AP operation mode            : Normal
Maximum Number of Radios     : 1
Current Number of Radios     : 1
Client Keep-alive Interval   : Disable
Client Idle Interval(s)      : 3600
Broadcast-probe Reply Status : Enable
Radio 1:
  Basic BSSID                : 000f-e2cd-0930
  Current BSS Count          : 5
  Running Clients Count      : 0
  Wireless Mode              : 11g
  Configured Channel         : auto(1)
  Configured Power (dBm)     : 10
  Preamble Type              : short
  Radio Policy               : default-rp
  Service Template           : 1    (SSID: h3c-igmp)
  Service Template           : 2    (SSID: h3c-wpa)
  Service Template           : 4    (SSID: h3c-wpa-psk)
  Service Template           : 3    (SSID: test)
  Service Template           : 5    (SSID: dot1x)
  Admin State                : UP
  Physical State             : UP
  Operational Rates (Mbps):
    1                        : mandatory
    2                        : mandatory
    5.5                      : mandatory
    6                        : supported
    9                        : supported
    11                       : mandatory
    12                       : supported
    18                       : supported
    24                       : supported
    36                       : supported
    48                       : supported
    54                       : supported
  Radar detected Channels    : None
```

四、 MA5200的配置

1) 创建名为zlb的地址池

[MA5200F] **ip pool zlb local**

[MA5200F-ip-pool- zlb] **gateway 192.168.1.1 255.255.255.0**

[MA5200F-ip-pool- zlb] **section 0 192.168.1.10 192.168.1.200**

2) 新建认证方案auth1和计费方案acc1

[MA5200F] **aaa**

[MA5200F-aaa] **authentication-scheme auth1**

[MA5200F-aaa-authen-auth1] **authentication-mode radius**

[MA5200F] **aaa**

[MA5200F-aaa] **accounting-scheme acct1**

[MA5200F-aaa-accounting-acct1] **accounting-mode radius**

3) 配置radius认证服务器

[MA5200F]**radius-server group radius-group1**

[MA5200F-radius-radius1] **radius-server authentication 192.168.0.100 1812**

[MA5200F-radius-radius1] **radius-server accounting 192.168.0.100 1813**

[MA5200F-radius-radius1] **radius-server key h3c**

[MA5200F-radius-radius1] **radius-server type portal**

4) 配置web认证服务器

[MA5200F] **web-auth-server 192.168.0.100 key h3c**

5) 配置认证前的域default0

[MA5200F-aaa-domain-default0] **ip-pool zlb**

[MA5200F-aaa-domain-default0] **ucl-group 1**

[MA5200F-aaa-domain-default0] **web-server 192.168.0.100**

[MA5200F-aaa-domain-default0] **web-server url**

http://192.168.0.100/portal

6) 配置认证时的域isp

[MA5200F] **aaa**

[MA5200F-aaa] **domain isp**

[MA5200F-aaa-domain-isp] **authentication-scheme auth1**

[MA5200F-aaa-domain-isp] **accounting-scheme acct1**

[MA5200F-aaa-domain-isp] **radius-server group radius-group1**

7) 配置系统的ACL策略

[MA5200F] **acl number 3000 match-order auto**

[MA5200F-acl-adv-3000] **rule user-net permit ip source 1 destination**

192.168.0.100 0

[MA5200F-acl-adv-3000] **rule net-user permit ip source 192.168.0.100 0 destination 1**

[MA5200F-acl-adv-3000] **rule user-net deny ip source 1**

[MA5200F] **access-group 3000**

8) 配置VLAN端口

[MA5200F] **portvlan ethernet 2 vlan 0 2**

[MA5200F-ethernet2-2-vlan0-1] **access-type layer2-subscriber**

[MA5200F-ethernet2-2-vlan0-1] **default-domain authentication isp**

[MA5200F-ethernet2-2-vlan0-1] **authentication-method web**

9) 配置上行接口

[MA5200F] **portvlan ethernet 1 vlan 0 1**

[MA5200F-ethernet1-1-vlan0-0] **access-type interface**

[MA5200F] **interface Ethernet 1.0**

[MA5200F-Ethernet1.0] **ip address 192.168.0.2 255.255.255.0**

MA5200F的完整配置如下：

```
#
 version 7149
 sysname MA5200F
#
 system language-mode english
#
 FTP server enable
#
 web-auth-server version v2
 web-auth-server 192.168.0.100 key h3c
#
radius-server group radius-group1
 radius-server key h3c
 radius-server authentication 192.168.0.100 1812
```

```
 radius-server accounting 192.168.0.100 1813
 radius-server traffic-unit kbyte
radius-server group radius
radius-server group login
#
 undo trap-statistics 7242002
 undo trap-statistics 7242003
 undo trap-statistics 70f2000
 undo trap-statistics 70f2001
 undo trap-statistics 70f2002
 undo trap-statistics 70f2003
 undo trap-statistics 70f2004
 undo trap-statistics 70f2005
 undo trap-statistics 70f2008
 undo trap-statistics 70f2009
 undo trap-statistics 70f200c
 undo trap-statistics 70f200d
 undo trap-statistics 70f200e
 undo trap-statistics 70f200f
 undo trap-statistics 70f2017
 undo trap-statistics 70f2018
 undo trap-statistics 70f201c
 undo trap-statistics 70f201d
 undo trap-statistics 7032000
 undo trap-statistics 7032001
 undo trap-statistics 7032002
#
 login local-user zlb  password simple zlb
#
interface Ethernet1
#
interface Ethernet2
#
interface Ethernet3
#
interface Ethernet4
#
interface Ethernet5
#
interface Ethernet6
#
interface Ethernet7
#
interface Ethernet8
#
interface Ethernet9
#
interface Ethernet10
#
interface Ethernet11
#
interface Ethernet12
#
interface Ethernet13
#
interface Ethernet14
#
interface Ethernet15
#
interface Ethernet16
#
interface Ethernet17
#
interface Ethernet18
```

```
#
interface Ethernet19
#
interface Ethernet19.0
 ip address 192.168.0.200 255.255.255.0
#
interface Ethernet20
#
interface Ethernet21
#
interface Ethernet22
#
interface Ethernet23
#
interface Ethernet24
#
interface GigabitEthernet25
#
interface GigabitEthernet26
#
interface NULL0
#
interface LoopBack0
#
interface Nm-Ethernet0

acl number 3001
 rule 1 net-user permit ip source 192.168.0.100 0 destination 1
 rule 0 user-net permit ip source 1 destination 192.168.0.100 0
 rule 2 user-net deny ip source 1
#
l2tp-group 1
#
ip pool zlb local
 gateway 192.168.1.1 255.255.255.0
 section 1 192.168.1.10 192.168.1.200
#
dot1x-template 1
#
aaa
authentication-scheme  auth1
accounting-scheme  acc1
 accounting realtime  3
domain  default0
 web-server  192.168.0.100
 web-server url  http://192.168.0.100/portal
 ucl-group   1
 ip-pool   zlb
domain  isp
 authentication-scheme   auth1
 accounting-scheme   acc1
 radius-server group  radius-group1
#
local-aaa-server
 local-accounting alarm-threshold flash 100
#
 ip route-static 0.0.0.0 0.0.0.0 192.168.0.100
#
 access-group 3001
#
user-interface con 0
user-interface vty 0 4
#
portvlan ethernet 19 vlan 0 1
```

access-type interface

portvlan ethernet 20 vlan 0 2

access-type layer2-subscriber

default-domain authentication isp

authentication-method web

#

return

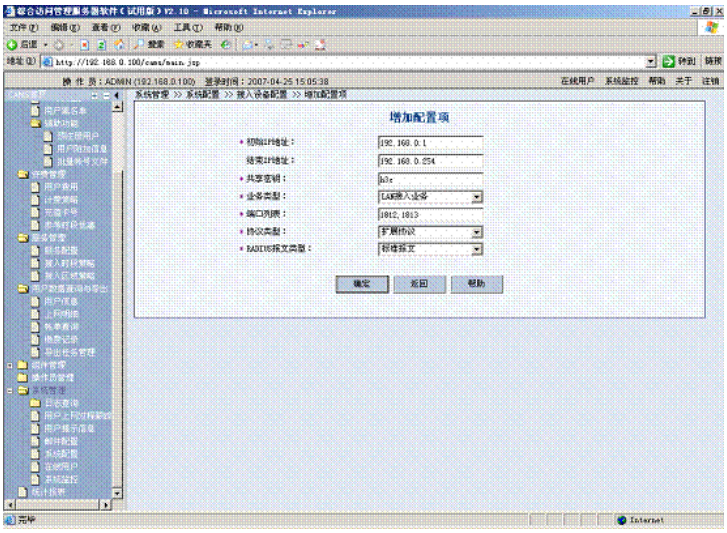
五、 Cams的相关配置

1、在CAMS系统的“**系统管理>>系统配置>>接入设备配置>>增加配置项**”中进行如下图所示配置。

·保证交换机的IP地址在配置的初始IP地址和结束IP地址的范围内（如192.168.0.2在192.168.0.1 - 192.168.0.254的范围内）。

·保证共享密钥中的配置与交换机的radius-server中的配置一致（如本例中为*h3c*）。

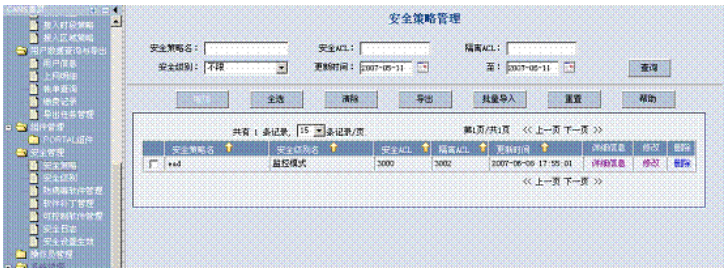
·保证端口列表中的配置与交换机的radius-server中的配置一致（如本例中为*1812，1813*）。



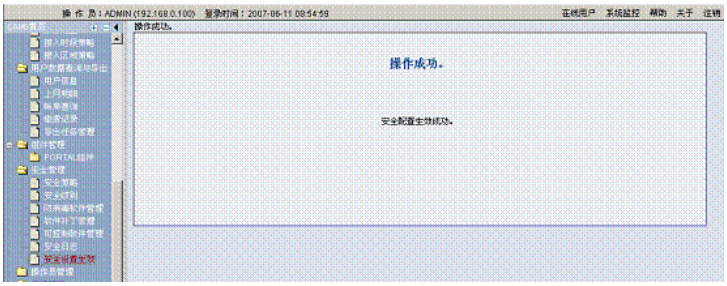
2、在CAMS系统的“**安全管理>>安全策略>>增加安全策略**”中进行如下图所示配置。（本例中使用的安全策略名为ead）

其中的隔离ACL和安全ACL在交换机上定义。其他安全检查和安全策略在“防病毒软件管理”，“软件补丁管理”，“可控软件管理”中配置。

“隔离ACL”和“安全ACL”不需要填写，即不下发ACL，否则会造成认证不通过。



设置完“安全策略”后，要点击“安全设置生效”。



3．在CAMS系统中PORTAL组件的相关配置如下：

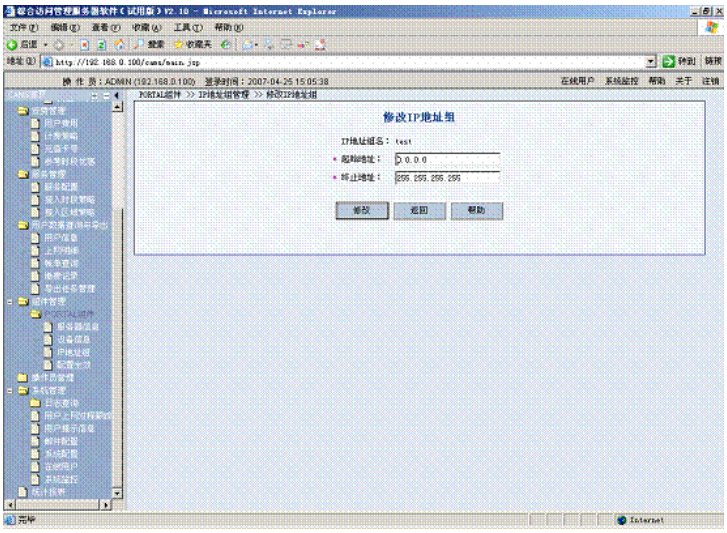
PORTAL服务器信息如下图所示。

服务器IP地址：192.168.0.100

PORTAL主页：http://192.168.0.100/portal

“服务类型列表”中添加Portal服务所代表的域名。通过“服务类型表识”项增加，如本实验的域名“isp”。“服务类型描述”是对其的标称，在客户端iNode认证街面上会显示此名字，如果选择上，表示客户端带域名认证，即用户名带”isp”域名认证。

IP地址组信息设置：



配置设备端口组信息设置：

点击生效，使配置生效：

4．在CAMS系统的“**服务管理>>服务配置>>增加服务**”中进行如下图所示配置。（本例中使用的服务名为*hx*）

“服务后缀”中，填写域名，这里填写域名“isp”。

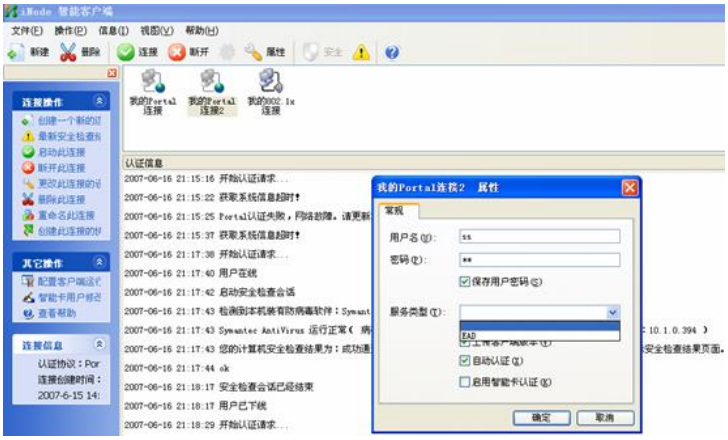
5．在CAMS系统的“**用户管理>>帐户用户>>用户开户**”中进行如下图所示配置。（本例中帐户名为*hx*，密码为*hx*，选择相应的服务*hx*）

六、　客户端的相关设置

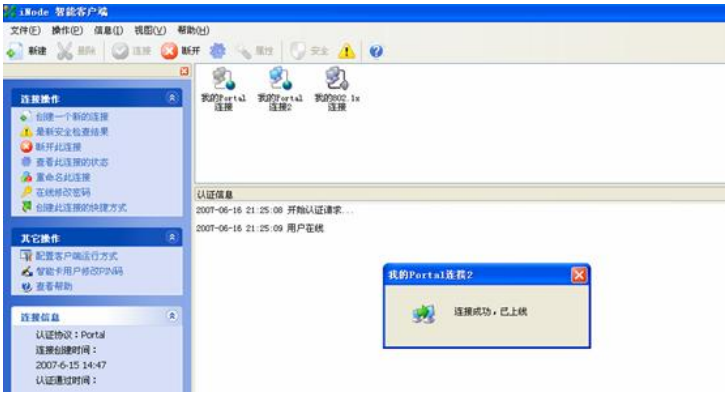
首先在Windows无线客户端中选择连接SSID ***Test***，。客户端连接成功后会自动获取IP地址。这时需要配置iNode 客户端，“服务类型”选择“EAD”

，用户带域名认证。

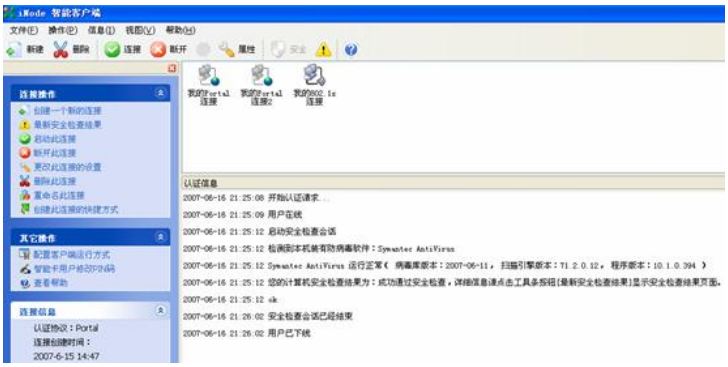
1）用户带域名认证



认证成功：



用户下线：



2）用户不带域名认证

不带域名的情况有如下几种情况：

1. MA5200上**radius-server**配置中加入命令：“**undo radius-server user-name domain-included**”。这样用户名即使带域名认证，也会在MA5200上被剥去。
2. 客户端“服务类型”不选择EAD方式，即表示域名的标识符。
3. Cams服务器的Portal服务器信息中，不配置“服务器类型列表”，这样iNode客户端的认证界面中，“服务类型”中就不会出现表示于面的EAD。
4. Cams配置中的服务不配置域名后缀，表示对应不带域名的用户。