

之前已经介绍过无线的认证了，包括 open 以及 WPA 的方式，这次介绍一个在企业网络中比较特殊的方式，基于客户的 MAC 地址认证，它必须实现知道客户端的 MAC 地址，然后在本地或者基于 radius 外部数据库的方式。

掌握目标

- 一、AC 的基本配置
- 二、测试是否正常拨入
- 三、基于本地 MAC 地址的方式
- 四、基于 radius

拓扑说明（省略）

这里拓扑很简单，具体配置都在 AC 上面，所以参考之前的拓扑即可。

一、AC 的基本配置

Dhcp enable

```
[Huawei-AC6605]int vlan 1
```

```
[Huawei-AC6605-Vlanif1]ip address 192.168.1.251 24
```

```
[Huawei-AC6605-Vlanif1]dhcp sel intaface
```

说明：配置一个 IP 地址，该接口地址用来与 AP 通信的。

```
[Huawei-AC6605]wlan
```

```
[Huawei-AC6605-wlan-view]wlan ac source interface Vlanif 1
```

```
[Huawei-AC6605-wlan-view]ap-auth-mode sn-auth
```

```
[Huawei-AC6605-wlan-view]ap id 1 type-id 19 sn 21023544831069236750
```

说明：定义了 AC 的源地址为 VLAN 1，该地址是与 AP 进行建立 CAPWAP 隧道的，启用了 AP 认证功能，使用序列号，然后在 AP 定义了一个 ID 为 1，然后 AP 类型为 19，序列号为那个。其中 type-id 是可以查看的，SN 则在 AP 上面查看。

```
<AC6605>display ap-type all
All AP types information:
-----
ID      Type
-----
0       WA601
1       WA631
2       WA651
3       WA602
4       WA632
5       WA652
6       WA603SN
7       WA603DN
8       WA633SN
11      WA603DE
12      WA653DE
14      WA653SN
17      AP6010SN-GN
18      WA615DN-AGN
19      AP6010DN-AGN
20      WA635SN-GN
21      AP6310SN-GN
22      WA655DN-AGN
23      AP6510DN-AGN
25      AP6610DN-AGN
27      AP7110SN-GN
28      AP7110DN-AGN
29      AP5010SN-GN
30      AP5010DN-AGN
31      AP3010DN-AGN
32      WA655DN-AGN-US
33      AP6510DN-AGN-US
34      AP6610DN-AGN-US
-----
Total number: 28
<AC6605>
```

可以通过 display ap-type all 查看该 AC 支持的 AP 类型，其中 AP6010DN ID 为 19，所以定义 ID 为 19，至于序列号怎

么查看，在 AP 上面通过 displa system-information 查看

```
<Huawei>display system-information
System Information
Serial Number       : 21023544831069236750
System Time        : 2014-06-09 13:11:36
System Up time     : 0:15
System Name        : Huawei
Country Code       : US
MAC Address        : 00:e0:fc:bd:2d:40
Radio 2.4GHz MAC Address : 00:e0:fc:bd:2d:40
Radio 5GHz MAC Address : 00:e0:fc:bd:2d:50
IP Address         : 169.254.1.1
Subnet Mask        : 255.255.0.0
Default Gateway    : 0.0.0.0
Management VLAN ID(AP) : 1
IP MODE            : dhcp
Slot Status        : Dual band(an/bgn)
AP Type            : AP6010DN-AGN
Board Type         : AP6010DN
Board Serial Number : 
Board Bom Version  : 0
Boot Rom Version   : -
Software Version   : V200R003C00
Hardware Version    : H86D2TD1D200 VER.A
Telnet Access      : 
User Name          : admin
=====
```

结果验证

```
<Huawei>display ip int br
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 2
The number of interface that is DOWN in Physical is 0
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 0

Interface          IP Address/Mask      Physical  Protocol
NULL0              unassigned           up        up(s)
Vlanif1            169.254.1.1/16       up        up

<Huawei>
```

目前来看，AP 还没有获取到地址，这个是定期发送 DHCP 报文获取的。

```

<Huawei>
<Huawei>display ip int br
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 2
The number of interface that is DOWN in Physical is 0
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 0

Interface                IP Address/Mask      Physical  Protocol
NULL0                    unassigned           up        up(s)
Vlanif1                  192.168.1.201/24     up        up

<Huawei>
<Huawei>
<Huawei>
===== CAPWAP LINK IS UP!!! =====

<Huawei>
<ap-1>

```

通过查看已经获取到了 IP 地址了，然后即可与 AC 建立 CAPWAP 隧道，这个过程需要一定的时间，后面可以看到 CAPWAP 隧道已经建立了

```

<ap-1>display capwap link state
-----
LINK          AP      AP      AP      InIf      FSM
ID            IPAddr CPort  DPort    Index     State
-----
0             192.168.1.201 50617 50618     0         RUN
-----
<ap-1>

```

查看隧道状态为 RUN。

```

<AC6605>display ap all
All AP information(Normal-1,UnNormal-0):
-----
AP      AP      AP      Profile  AP      AP
ID      Type      MAC      /Region  State  Sysname
-----
1       AP6010DN-AGN  00e0-fcbd-2d40  0/0     normal ap-1
-----
Total number: 1
<AC6605>

```

可以看到 AC 上面也有对应的 AP 信息了。至此 AP 上线完成。

.2、AC 配置第二部【定义 AP 域 、业务功能】

```
[Huawei-AC6605]wlan
```

```
[Huawei-AC6605-wlan-view]ap-region id 1
```

```
[Huawei-AC6605-wlan-ap-region-1]ap id 1
```

说明：默认存在一个与为 0，建议的是不同业务或者部门可以加入不同的域，这样的话后续调整射频参数、调优等参数则只影响该域的参数。

WMM 模板定义

WMM 模板是提供了 QOS 等服务等级，将数据报文按照优先级从高到低分为 4 个接入类 AC (Access Category)：AC_VO(语音)、AC_VI(视频)、AC_BE(尽力而为)、AC_BK(背景)，高优先级的 AC 占用信道的机会大于低优先级的 AC。

```
[Huawei-AC6605]wlan
```

```
[Huawei-AC6605-wlan-view]wmm-profile name Ap1
```

说明：WMM 默认情况下有默认策略的，没有特别需求的话，可以直接使用默认的。

射频模板定义

射频模板参数内容包括：射频类型、射频速率、射频信道模式、射频功率模式、丢包/错包率门限、冲突率门限、分段门限、RTS/CTS 门限、短/长帧最大重传次数门限、是否支持短前导码、DTIM 周期、beacon 帧周期、WMM 参数等。

```
[Huawei-AC6605-wlan-view]radio-profile name 2.4G
```

```
[Huawei-AC6605-wlan-radio-prof-2.4G]wmm-profile name ap1
```

```
[Huawei-AC6605-wlan-view]radio-profile name 5G
```

```
[Huawei-AC6605-wlan-radio-prof-5G]wmm-profile name ap1
```

```
[Huawei-AC6605-wlan-radio-prof-5G]radio-type 80211an
```

说明：这里模板默认情况下只需要调用 WMM 模板，其余的都有默认策略，比如默认情况下，信道模式为 Auto，也就是 AC 会自动根据 AP 周围的信道自动合理规划信道，射频类型等。这里定义 2 个是一个作为 2.4G 使用，另外一个使用 5G

安全模板定义

```
[Huawei-AC6605]wlan
```

```
[Huawei-AC6605-wlan-view]security-profile name open
```

```
[Huawei-AC6605-wlan-view]security-profile name pre-authen
```

```
[Huawei-AC6605-wlan-sec-prof-pre-authen]security-policy wpa2
```

```
[Huawei-AC6605-wlan-sec-prof-pre-authen]wpa2 authentication-method psk pass-phrase simple ccieh3c.taobao.com  
encryption-method ccmp
```

说明：安全模板定了 2 个，一个为 Open，即默认策略，也就是后续定义的 Guest，不进行认证，而后面定义了一个 pre-auten 则为 WPA2 进行密码认证，这个是给内部用的。

流量模板

流量模板可以实现为某个无线网络定制特定的优先级映射和流量监管功能。

```
[Huawei-AC6605]wlan
```

```
[Huawei-AC6605-wlan-view]traffic-profile name AP-1
```

说明：默认情况下流量模板下，有默认策略，比如 802.1P 映射，用户的限速、VAP 限速等功能，这里先使用默认的，后续需求的话在进

行调整。

8 定义 WLAN-ESS 接口

WLAN-ESS 接口类似于一个模板，它的作用主要给一个 AP 可以虚拟多个 VAP 出来，VAP 提供给不同的服务接入，而一个 VAP 对应一个 WLAN-BDSS 接口，而 WLAN-ESS 则是 WLAN-BDSS 属性模板，也就是 AC 动态创建一个 VAP，则自动创建一个 WLAN-BDSS，而属性则继承 WLAN-ESS 定义的。

```
[Huawei-AC6605]interface Wlan-Ess 1
```

```
[Huawei-AC6605-Wlan-Ess1]port hybrid untagged vlan 19
```

说明：创建了一个 WLAN-ESS 接口，并且允许了 VLAN 19 的流量不打标签进入该接口，默认情况下 VLAN 1 已经通过了，所以这里的流量即为 VLAN 19 与 1。当然该接口还可以部署其他策略，比如 dot1x、MAC 认证等功能，注意的是，V200R3 的版本是不需要启用 DHCP 功能的，默认就开启了。

定义 WLAN 服务集

服务集的功能就是来汇集之前定义的业务参数功能，比如定义 SSID，转发模式，关联射频模板，认证策略等，然后调用在 AP 下，进行下发。

```
[Huawei-AC6605]wlan
```

```
[Huawei-AC6605-wlan-view]service-set name open
```

```
[Huawei-AC6605-wlan-service-set-open]ssid Guest
```

```
[Huawei-AC6605-wlan-service-set-open]forward-mode direct-forward
```

```
[Huawei-AC6605-wlan-service-set-open]wlan-ess 1
```

```
[Huawei-AC6605-wlan-service-set-open]service-vlan 19
```

```
[Huawei-AC6605-wlan-service-set-open]security-profile name open
```

```
[Huawei-AC6605-wlan-service-set-open]traffic-profile name AP-1
```

```
[Huawei-AC6605-wlan-view]service-set name intrenet
```

```
[Huawei-AC6605-wlan-service-set-intrenet]ssid intrent
```

```
[Huawei-AC6605-wlan-service-set-intrenet]service-vlan 19
```

```
[Huawei-AC6605-wlan-service-set-intrenet]wlan-ess 1
```

```
[Huawei-AC6605-wlan-service-set-intrenet]security-profile name pre-authen
```

```
[Huawei-AC6605-wlan-service-set-intrenet]forward-mode direct-forward
```

```
[Huawei-AC6605-wlan-service-set-intrenet]traffic-profile name AP-1
```

说明：这里创建了 2 个服务集，一个用于 Guest 用的，一个用于 intrenet，除了 SSID 与安全策略不一样外，其余的都一致。

射频配置

每个 AP 都有一个或多个射频模块，这个射频模块负责无线信号的收发、功率的调整以及信道的配置等功能。

```
[Huawei-AC6605]wlan
```

```
[Huawei-AC6605-wlan-view]ap 1 radio 0
```

```
[Huawei-AC6605-wlan-radio-1/0]radio-profile name 2.4G
```

```
[Huawei-AC6605-wlan-radio-1/0]service-set name open
```

```
[Huawei-AC6605-wlan-view]ap 1 radio 1
```

```
[Huawei-AC6605-wlan-radio-1/1]radio-profile name 5G
```

```
[Huawei-AC6605-wlan-radio-1/1]service-set name intrenet
```

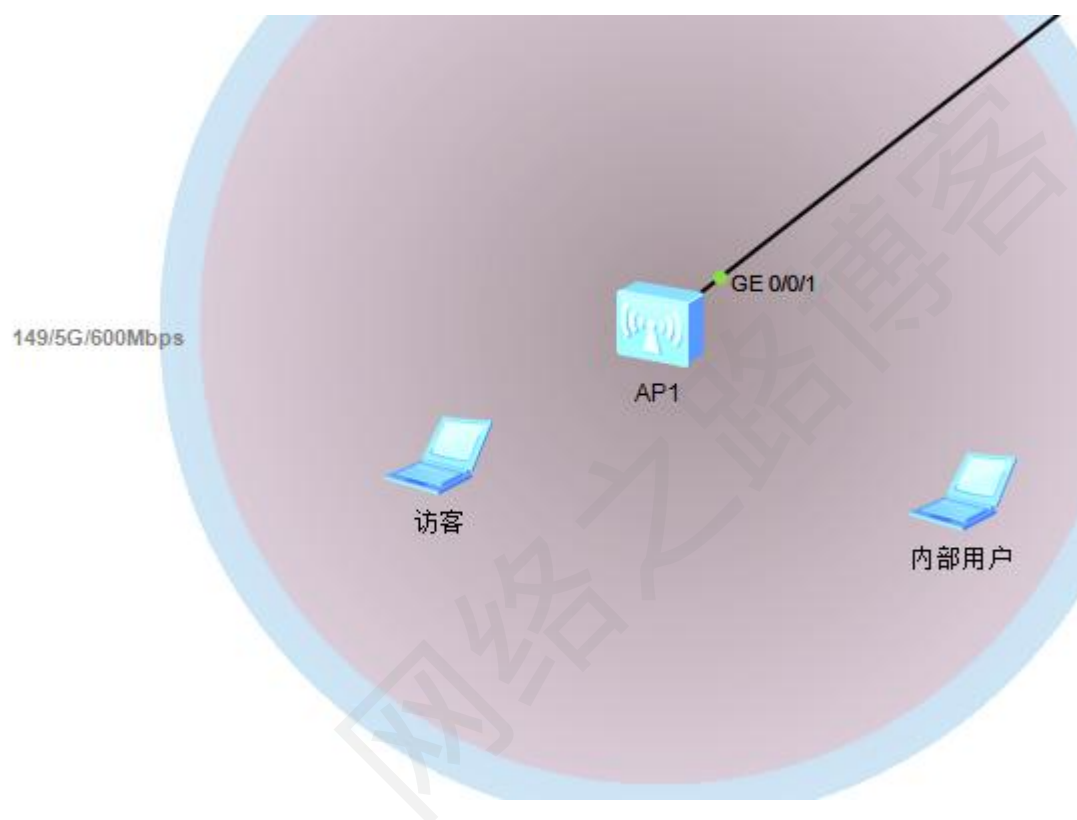
说明：这里定义了 2 个射频，一个给 2.4G 用，另外一个给 intrenet，2.4G 主要提供给 Guest 使用，而 5G 在内企业网内部

使用，这里说明的是，radio 0 为 2.4G 频率，而 1 为 5G 频率。

AC 配置第三步【下放业务配置给 AP】

```
[Huawei-AC6605-wlan-view]commit ap 1
```

8.4 环境测试验证



Vap 列表

命令行

UDP发包工具

MAC 地址:

54-89-98-E3-09-8C

IPv4 配置

☐ 静态☒ DHCP

IP 地址:

. . .

子网掩码:

. . .

网关:

. . .

Vap 列表

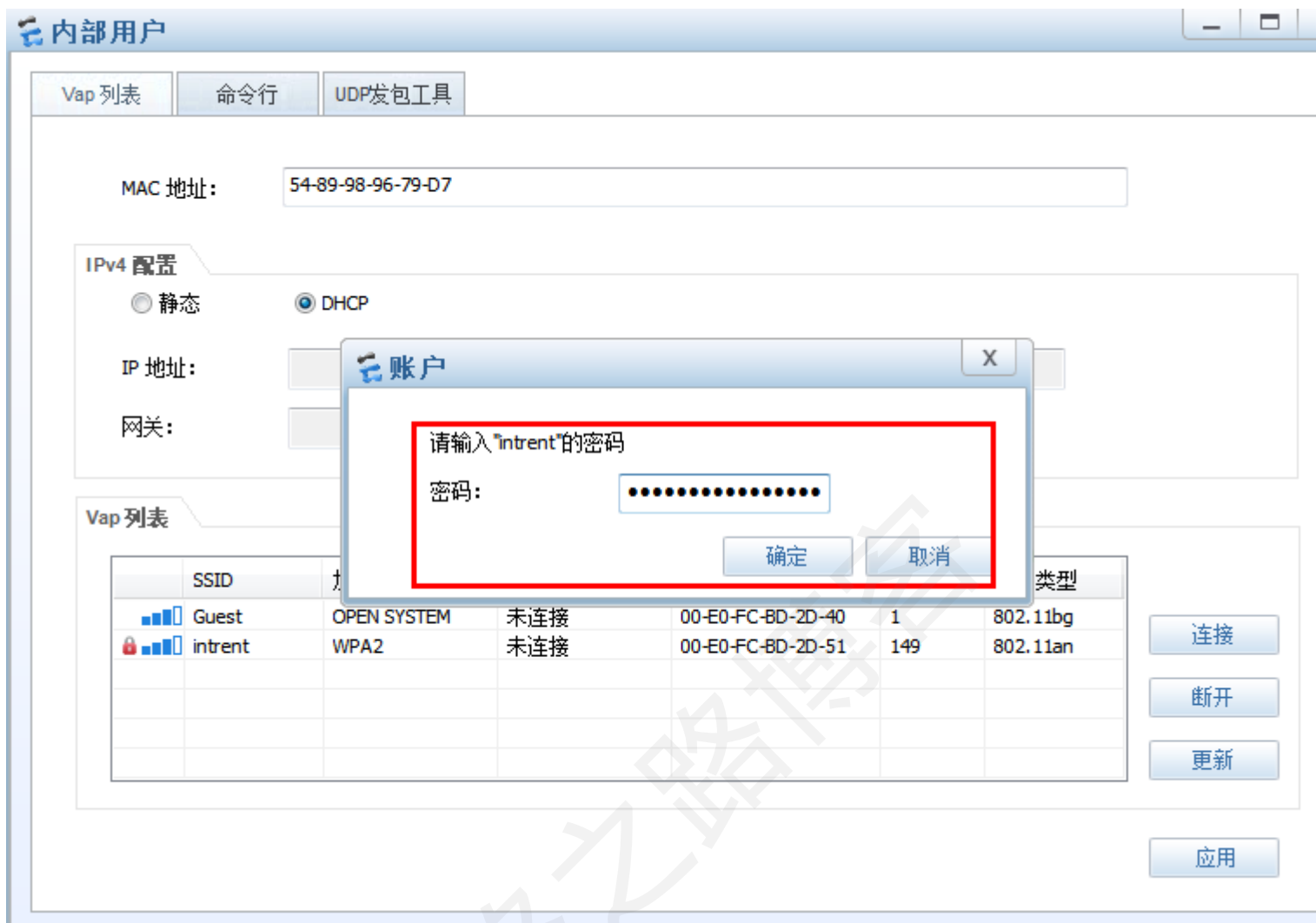
	SSID	加密方式	状态	VAP MAC	信道	射频类型
	Guest	OPEN SYSTEM	已连接	00-E0-FC-BD-2D-40	1	802.11bg
	intrent	WPA2	未连接	00-E0-FC-BD-2D-51	149	802.11an

连接


断开

更新

应用



可以看到 2 个客户端都已经连接上去了，默认情况下访客是不需要用户名密码认证，而内部用户则需要。

 访客

Vap 列表

命令行

UDP发包工具


```
Welcome to use STA Simulator!

STA>Welcome to use STA Simulator!

STA>
STA>ipconfig

Link local IPv6 address.....: ::
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 192.168.19.3
Subnet mask.....: 255.255.255.0
Gateway.....: 192.168.19.254
Physical address.....: 54-89-98-E3-09-8C
DNS server.....: 192.168.8.251

STA>
```

 内部用户

Vap 列表

命令行

UDP发包工具

```
Welcome to use STA Simulator!

STA>ipconfig

Link local IPv6 address.....: ::
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 192.168.19.4
Subnet mask.....: 255.255.255.0
Gateway.....: 192.168.19.254
Physical address.....: 54-89-98-96-79-D7
DNS server.....: 192.168.8.251

STA>
```

可以看到已经正常获取到 IP 地址了。

(8) 无线 MAC 认证功能

说明：在有时候我们希望这用对客户的 PC 做确认，用 MAC 地址进行认证登陆，而认证方式则 Open 的，那么我们需要开启 MAC 认证功能，该功能对客户来说是透明的，也就是说客户只要 MAC 地址符合要求，则看起来没有经过认证的样子，直接关联登陆了，而不在对应的列表内的话，则直接关联不上。

(1) 直接调用之前的 Open 的策略

说明：之前有策略存在，所以这里直接调用即可，先把服务集在 ap 1 中去掉。

(2) 开启 MAC 地址功能

```
[Huawei-AC6605]mac-authen
```

(3) WLAN-ESS 接口开启 mac-auth 功能

```
[Huawei-AC6605]interface Wlan-Ess 0
```

```
[Huawei-AC6605-Wlan-Ess0]mac-authentication enable
```

```
[Huawei-AC6605-Wlan-Ess0]force-domain default
```

```
[Huawei-AC6605-Wlan-Ess0]permit-domain default
```

说明：这里在 WLAN-ESS 接口开启 MAC 认证，并且必须指定从哪个域来的，然后允许。

(4) 本地定义用户名密码。

```
[Huawei-AC6605]aaa
```

```
[Huawei-AC6605-aaa]local-user 548998283f0e password cipher 548998283f0e
```

说明：注意转换为小写。

(5) 调用在服务集下【调用 WLAN-ESS】

说明：直接调用在 WLAN-ES 下就行了

(6) 下放业务

```
[Huawei-AC6605-wlan-view]commit all
```

(7) 结果测试

```
<AC6605>display mac-authen
MAC address authentication is Enabled.
Username format: use MAC address without-hyphen as username
Quiet period is 60s
Offline detect period is 300s
Server response timeout value is 30s
Reauthenticate period is 1800s
Guest user reauthenticate period is 60s
Maximum users: 128
Current users: 1
Global domain is not configured

wlan-Ess0 state: UP. MAC address authentication is enabled
Maximum users: 128
permit-domain default
force-domain default

wlan-Dbss0:0 status: UP
Authentication Success: 8, Failure: 5
Guest VLAN is disabled
Restrict VLAN is disabled

Online user(s) info:
-----
UserId   MAC/VLAN      AccessTime      UserName
-----
29       5489-9828-3f0e/19  2014/06/15 13:34:27  548998283f0e
-----
Total 1,1 printed
<AC6605>
```

已经成功了。有正常认证的。

四、Radius 配置定义

Radius 服务器定义，与 AAA，Domain

```
[Huawei-AC6605]radius-server template mac-authen
```

```
[Huawei-AC6605-radius-dot1x]radius-server authentication 192.168.2.253 1812
```

```
[Huawei-AC6605-radius-dot1x]radius-server shared-key test
```

```
[Huawei-AC6605-radius-dot1x]undo radius-server user-name domain-included
```

[Huawei-AC6605]aaa

[Huawei-AC6605-aaa]authentication-scheme mac-authen

[Huawei-AC6605-aaa-authen-dot1x]authentication-mode radius

[Huawei-AC6605-aaa]domain ccieh3c.taobao.com

[Huawei-AC6605-aaa-domain-ccieh3c.taobao.com]authentication-scheme mac-authen

[Huawei-AC6605-aaa-domain-ccieh3c.taobao.com]radius-server mac-authen

[Huawei-AC6605]interface Wlan-Ess 0

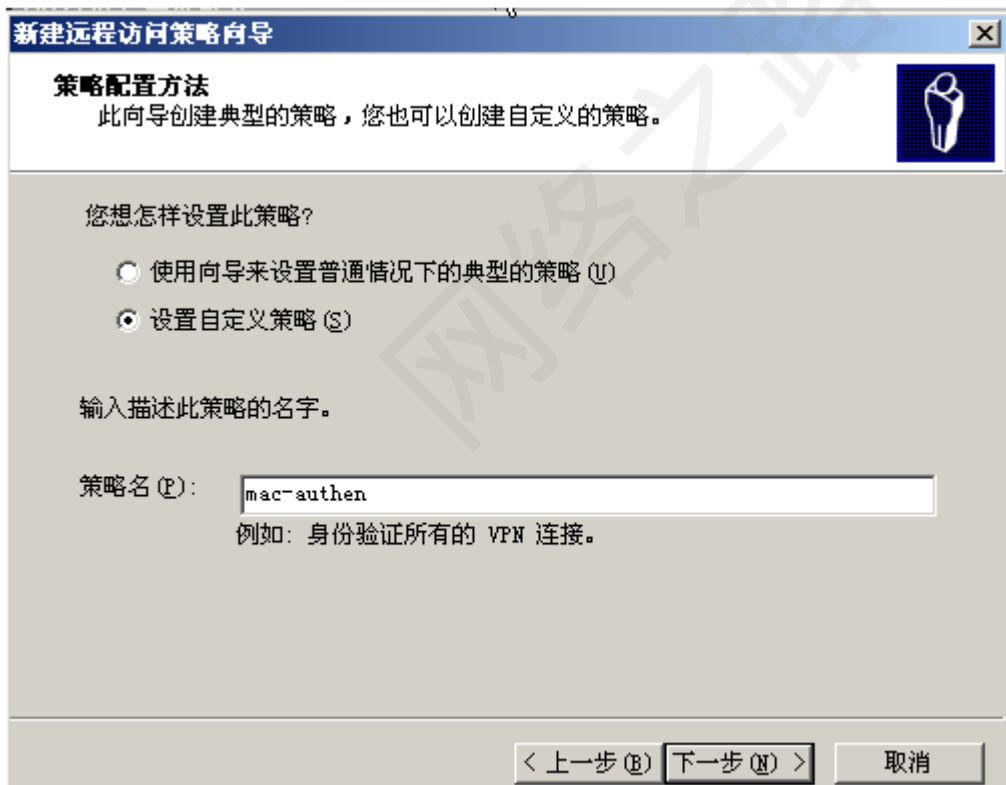
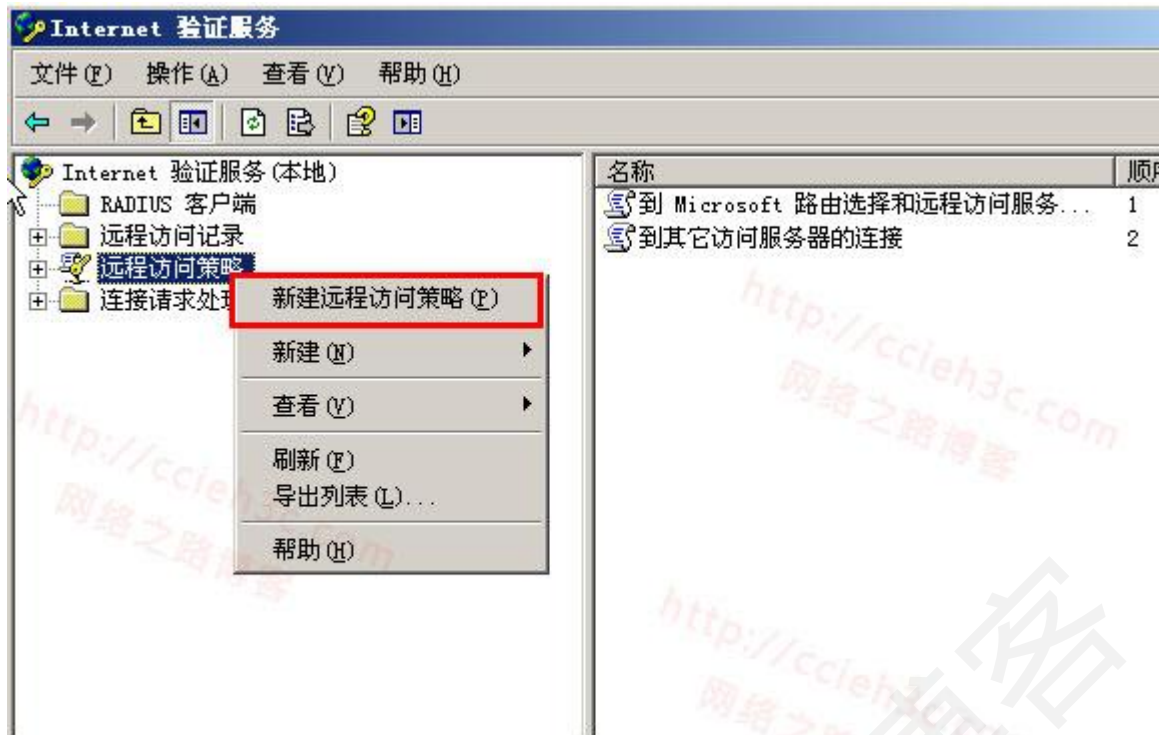
[Huawei-AC6605-Wlan-Ess0]mac-authentication enable

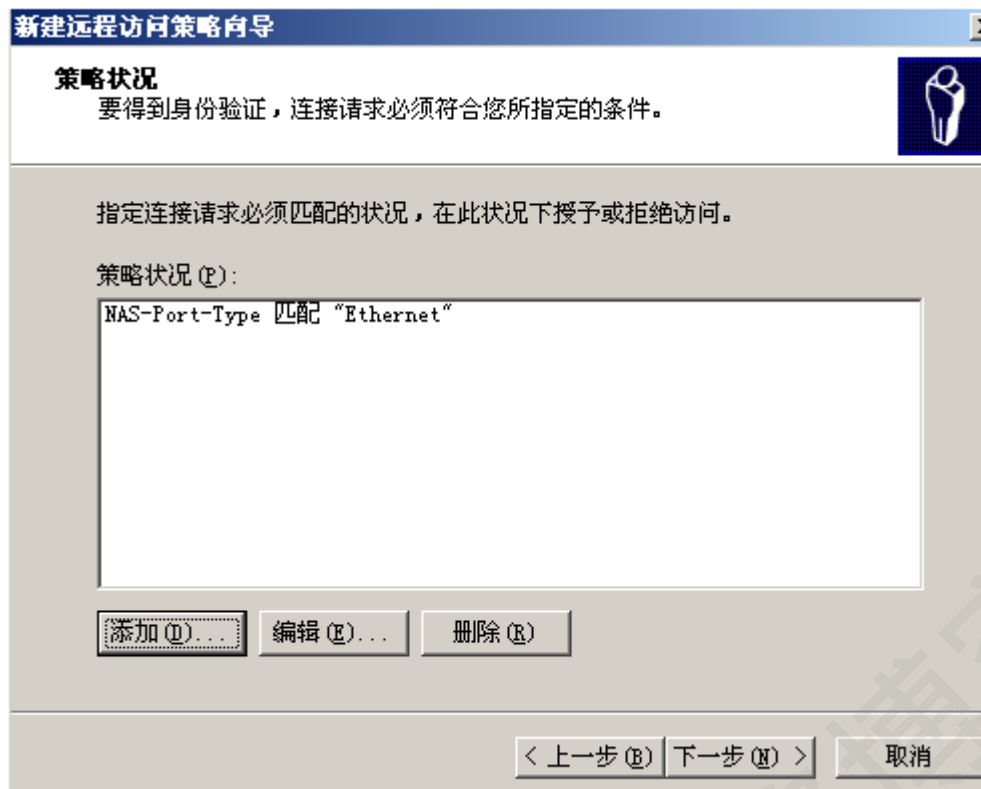
[Huawei-AC6605-Wlan-Ess0]force-domain mac-authen

[Huawei-AC6605-Wlan-Ess0]permit-domain mac-authen

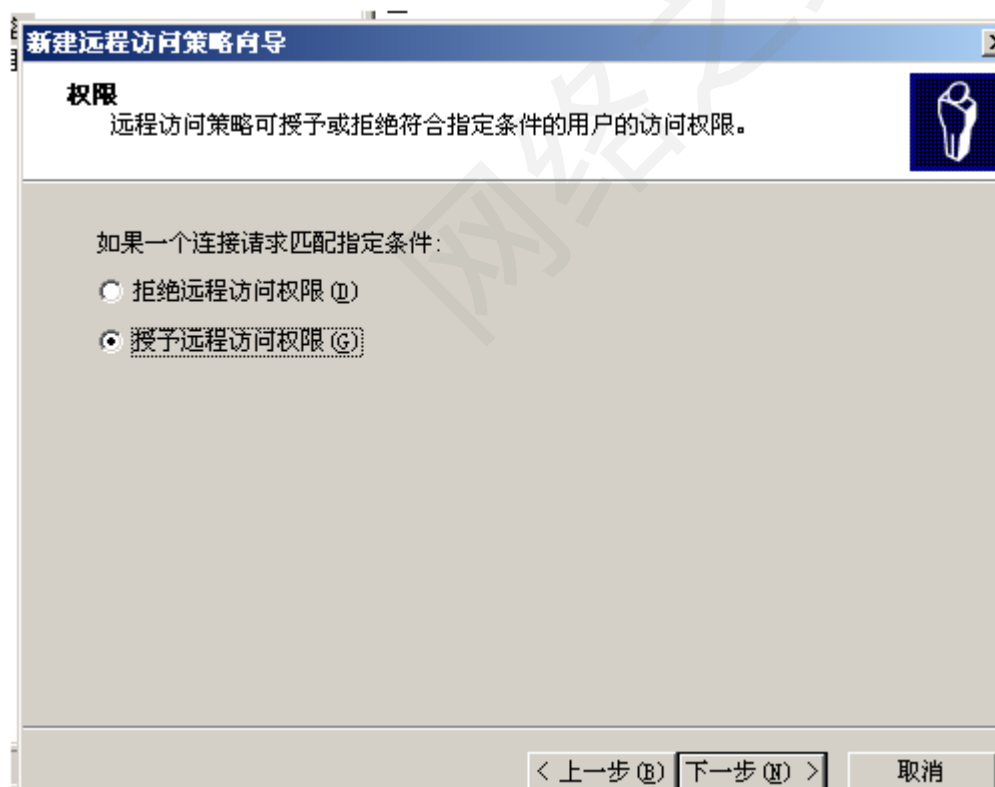
说明：这个需要把服务集去掉，然后去掉关来呢，然后才能设置 WLAN-ESS 接口，最后在关联。

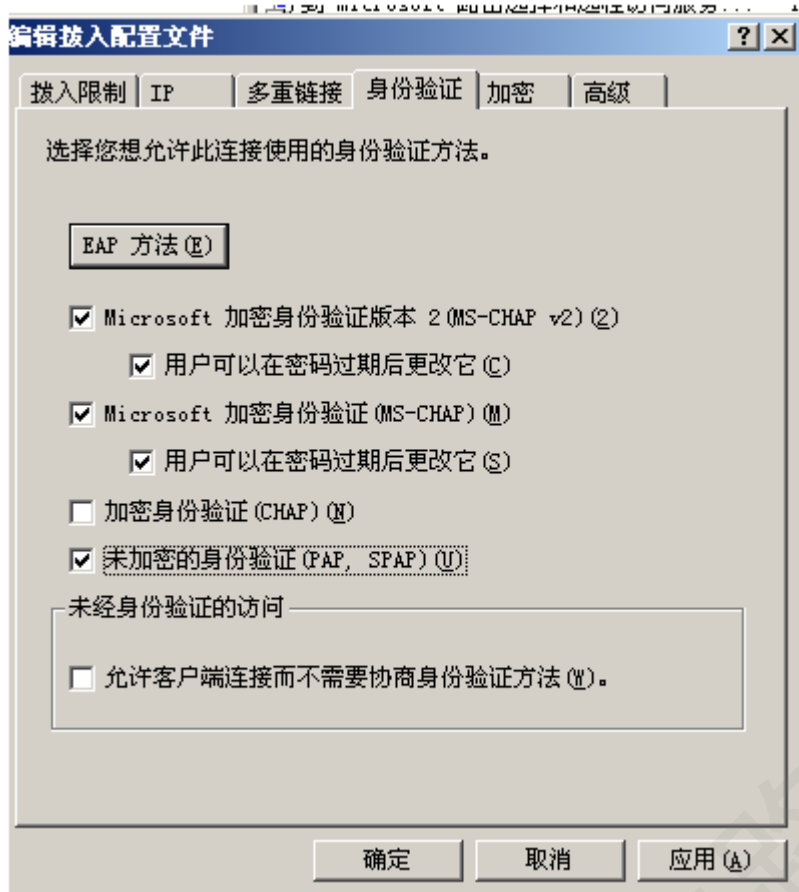
服务器配置





这里说明，是演示环境，所以直接匹配任何用户，然后匹配以太网类型即可。





```
Ethernet adapter 本地连接:

Connection-specific DNS Suffix . : 
Description . . . . . : VMware Accelerated AMD PCNet Adapter
Physical Address. . . . . : 00-0C-29-C4-FE-FB
```

PC的MAC地址

新用户

用户名 (U): 000c29c4fefb

全名 (F):

描述 (D):

密码 (P): *****

确认密码 (C): *****

☐ 用户下次登录时须更改密码 (M)

☐ 用户不能更改密码 (S)

☐ 密码永不过期 (W)

☐ 帐户已禁用 (B)

创建 (C) 关闭 (O)

Radius服务器上定义客户端的密码与用户。

测试

由于模拟器不支持该方式，只支持本地的，所以这里没办法进行测试，配置方法是没错的。可以在模拟器上面进行测试就可以了，类似于这样

```
<S5700> test-aaa 000c29c4fefb 000c29c4fefb radius-template test pap
<S5700>
Info: Account test succeed.
<S5700>
```

AC 上面也可以进行 test 测试的

博主也只是业余时间写写技术文档，请大家见谅，大家觉得不错的话，可以推荐给朋友哦，博主会努力推出更好的系列文档的。如果大家有任何疑问或者文中有错误跟疏忽的地方，欢迎大家留言指出，博主看到后会第一时间修改，谢谢大家的

支持，更多技术文章尽在网络之路博客，<http://ccieh3c.com>。



您的支持，是我们努力收集与分享的最大动力



微信公众平台
订阅第一时间享受
最新文章更新通知

远程设备调试服务
有需要的朋友可以
加微信聊



更多联系方式

QQ : 1914756383

邮箱 : 1914756383@qq.com

微信 : ciscohuawei3c

博客地址: <http://ccieh3c.com>

远程调试服务 : <https://1914756383.taobao.com>