WX5002与Windows IAS配合实现同一SSID不同VLAN功能（即动态mac-vlan功能）的典型配置

宋斌 2008-08-20 发表

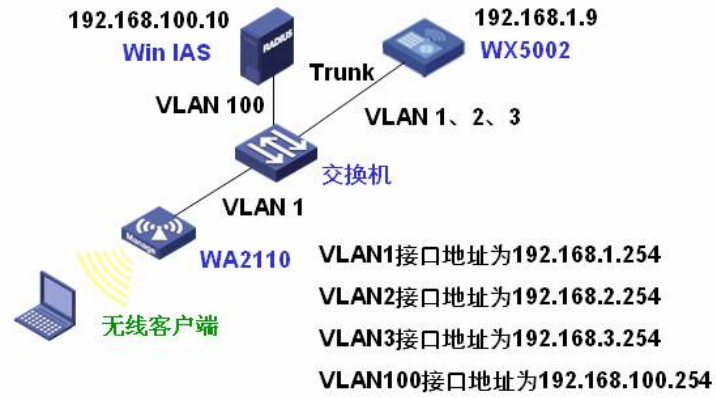
WX5002与Windows IAS配合实现同一SSID不同VLAN功能（即动态mac-vlan功能）的典型配置

适用WX5002版本：Comware Software, Version 5.20, Release 1106P02

一、组网需求

WX5002、WA2110、H3C POE交换机、便携机（安装有11b/g无线网卡）、Windows IAS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， WA2110在VLAN 1，WX5002和交换机之间为Trunk，通过VLAN1、2、3。

Windows IAS服务器在VLAN100，地址为192.168.100.10。

交换机上VLAN1、2、3、100的接口地址分别是192.168.1.254、192.168.2.254、192.168.3.254和192.168.100.254。

本例中WA2110的序列号为210235A22W0077000088。

SSID的名称为***H3C-mac-vlan***。

三、WX交换机的典型配置

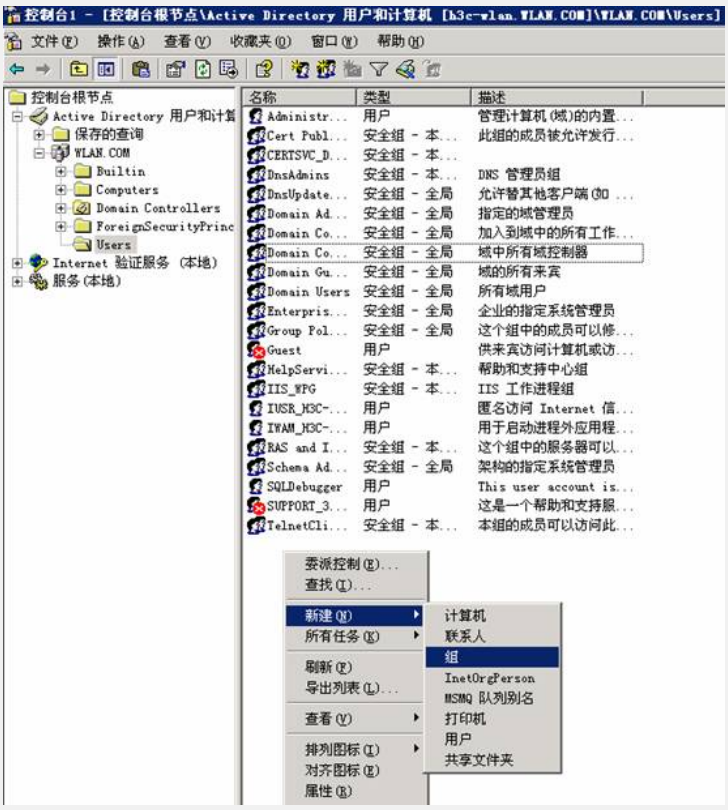
```
#
 version 5.20, Release 1106P02
#
 sysname H3C
#
 domain default enable isp
#
 port-security enable
#
 dot1x authentication-method eap
#
vlan 1
#
vlan 2 to 3
#
radius scheme radius1
 primary authentication 192.168.100.10
 primary accounting 192.168.100.10
 key authentication h3c
 key accounting h3c
 user-name-format without-domain
 nas-ip 192.168.1.9
#
domain isp
 authentication lan-access radius-scheme radius1
 authorization lan-access 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
#
dhcp server ip-pool 3
 network 192.168.3.0 mask 255.255.255.0
 gateway-list 192.168.3.254
 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 1 crypto
 ssid H3C-mac-vlan
 bind WLAN-ESS 1
 authentication-method open-system
 cipher-suite tkip
 security-ie wpa
 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
#
interface Vlan-interface3
 ip address 192.168.3.9 255.255.255.0
#
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-ESS1
 port link-type hybrid
 port hybrid vlan 1 to 3 untagged
 mac-vlan enable
```

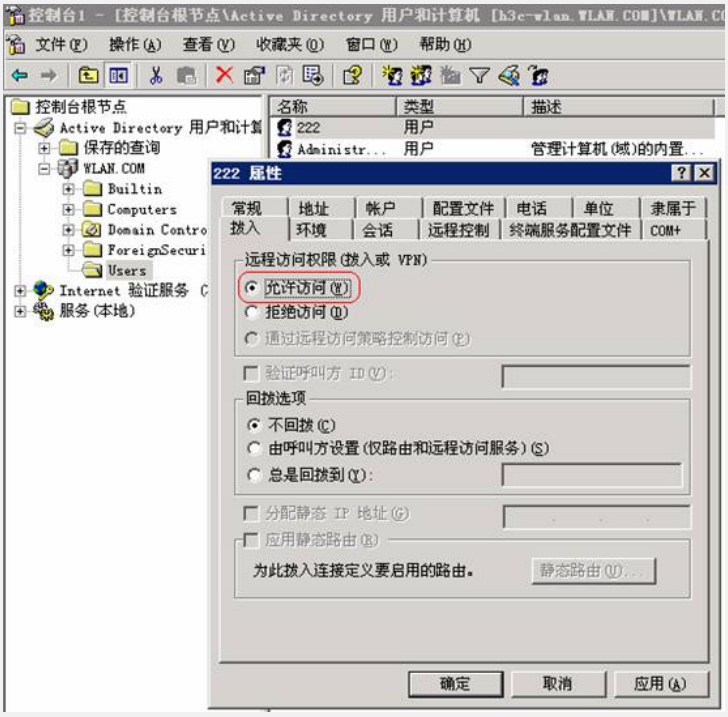
```
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
#
wlan ap ap1 model WA2100
 serial-id 210235A22W0077000088
 radio 1
  service-template 1
  radio enable
#
 ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
#
 dhcp enable
#
user-interface aux 0
user-interface vty 0 4
#
return
```

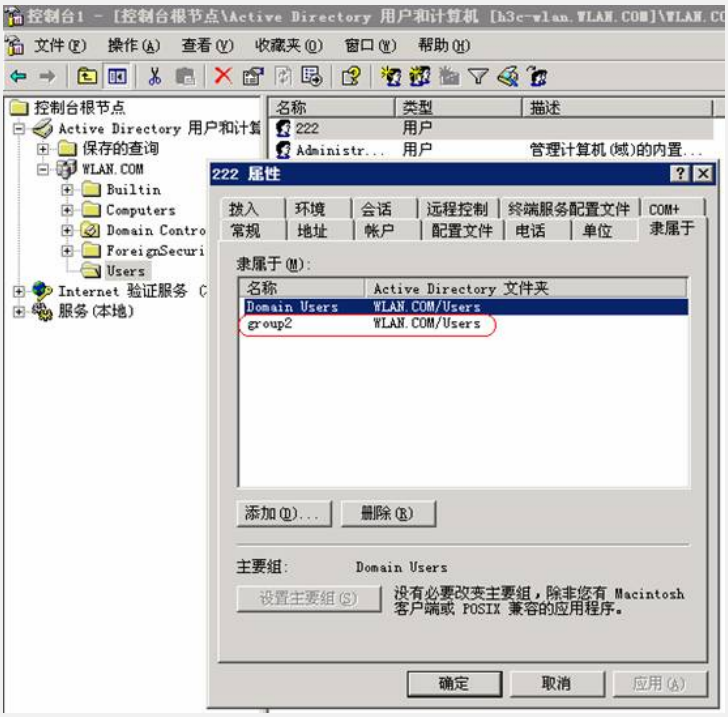
四、Windows AD (Active Directory) 的相关配置

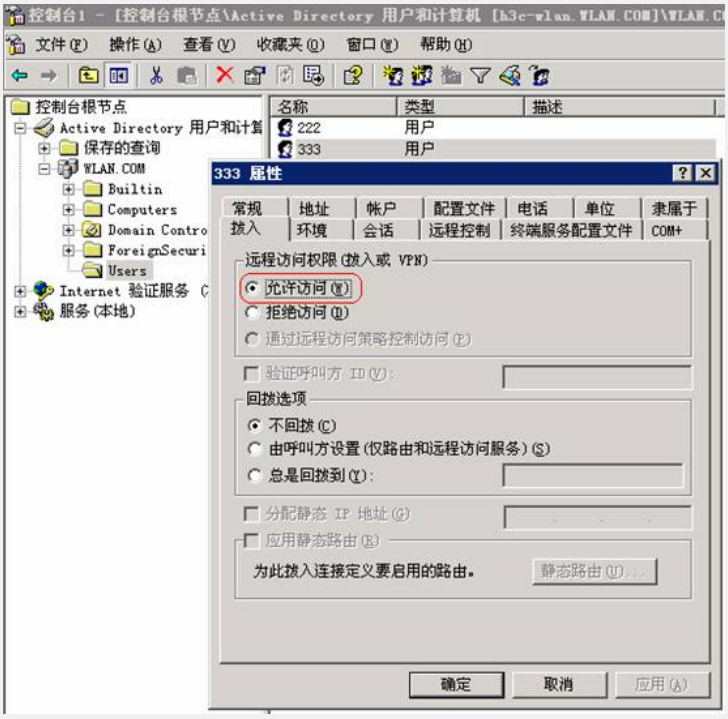
1、增加两个用户组**group2**和**group3**

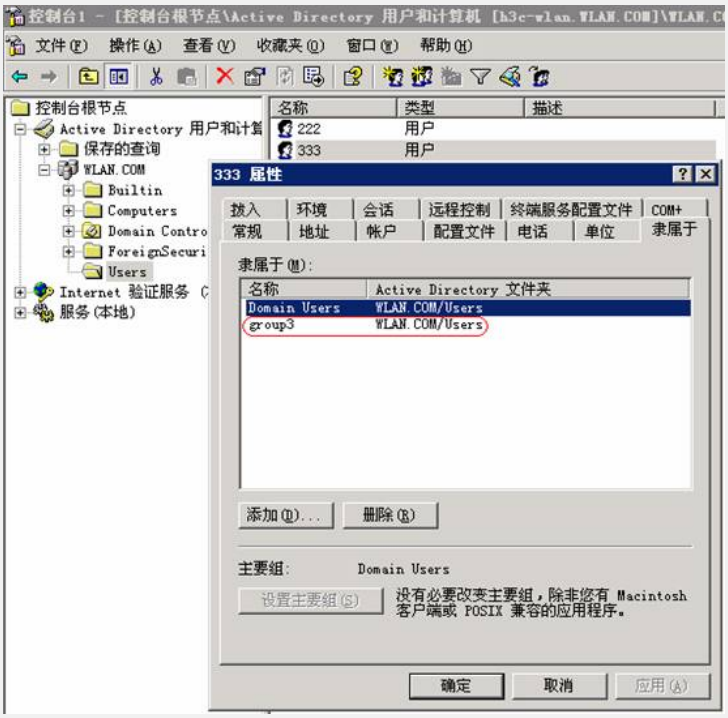


2、增加两个用户**222**和**333**，两个用户分别隶属于用户组**group2**和**group3**









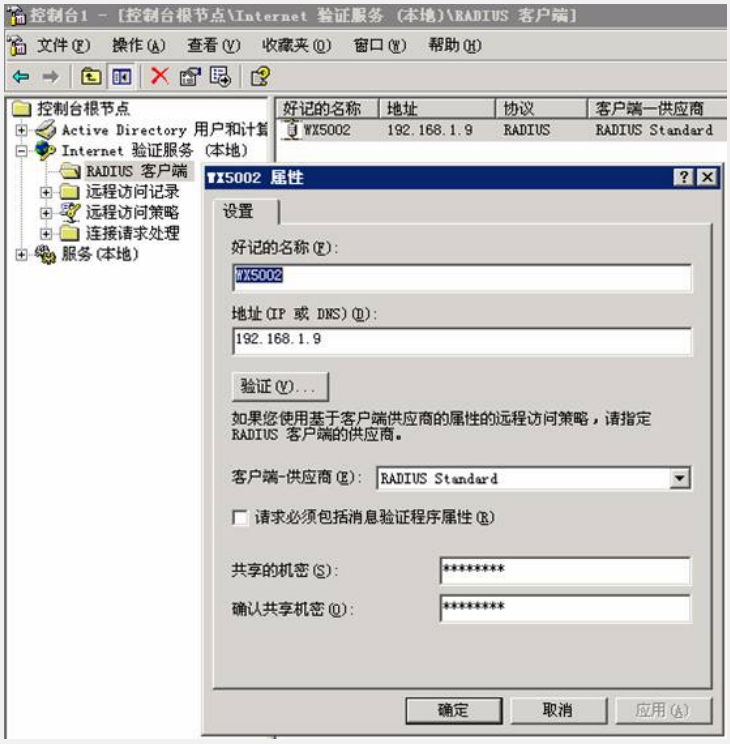
五、Windows IAS的相关配置

1、RADIUS客户端的相关配置

l 保证IP地址的配置与WX5002中的配置一致（如本例中为192.168.1.9）。

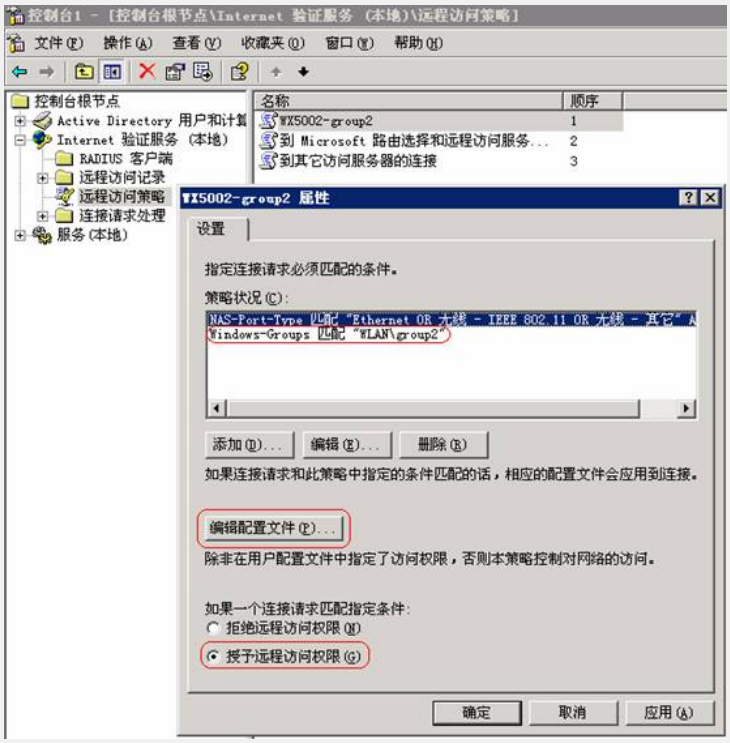
l 保证共享密钥中的配置与WX5002中的配置一致（如本例中为*h3c*）。

配置信息如下图所示：

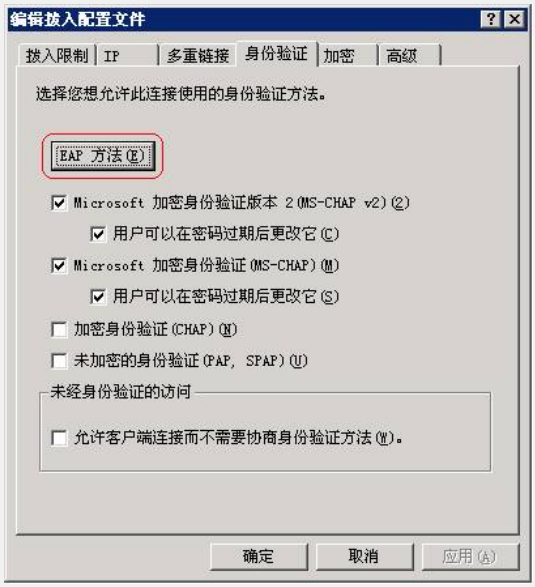


2、远程访问策略的相关配置

第一步：建立远程访问策略“WX5002-group2”,在策略状况中选择“**Windows-Groups 匹配‘WLAN\group2’**”，在使用的远程访问策略中选择“**授予远程访问权限**”，然后点击“**编辑配置文件**”，如下图所示

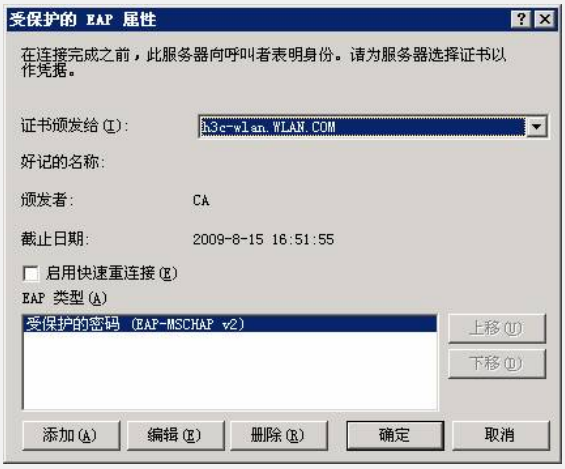


在“编辑配置文件”的对话框中选择“**EAP方法**”，如下图所示：



在“EAP方法”中选择“**受保护的EAP（PEAP）**”，如下图所示：

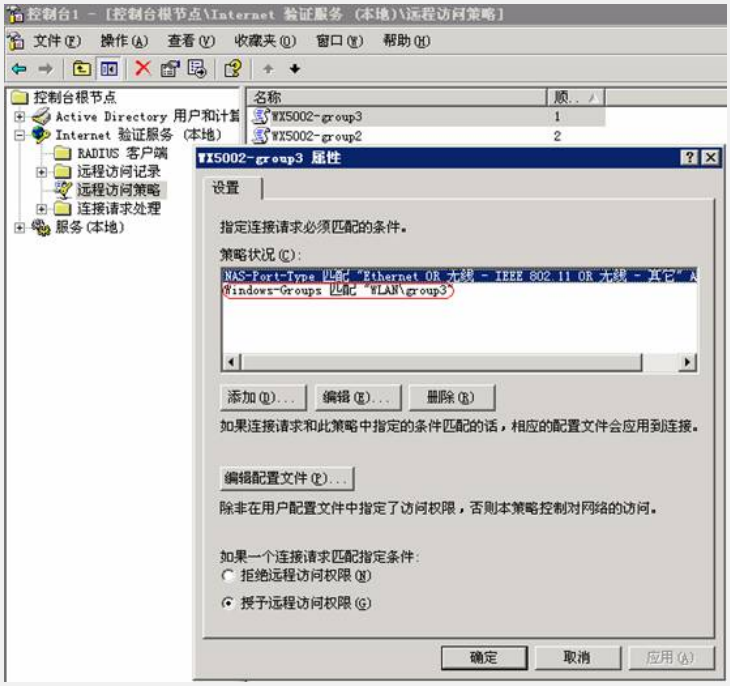
并在选中EAP方法后点击“**编辑**”，此EAP方法应处于可编辑状态，如下图所示：



第二步：在“**编辑配置文件**”的对话框中选择“**高级**”，在高级属性中需手动添加3个属性，分别是“**Tunnel-Medium-Type**”、“**Tunnel-Pvt-Group-ID**”、“**Tunnel-Type**”，各属性的内容如下图所示：

注：其中**Tunnel-Pvt-Group-ID**代表要下发的vlan号，采用“**十六进制方式**”，0x00000002代表下发的vlan id为2

第三步：建立远程访问策略“WX5002-group3”，在策略状况中选择“**Windows-Groups匹配‘WLAN\group3’**”，同时下发vlan id为3，其他属性与远程访问策略“WX5002-group2”相同，如下图所示：



六、Windows无线客户端的相关配置

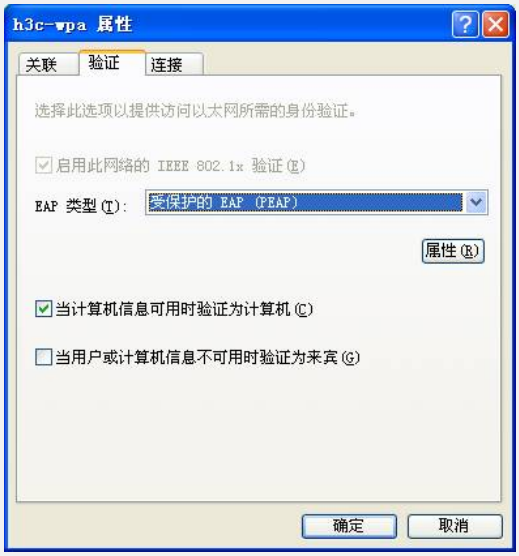
1、在Windows无线客户端中，通过“刷新网络列表”搜索相应的SSID，本例中的SSID

为“H3C-mac-vlan”，然后选择“更改高级设置”，如下图所示：

2、在弹出的对话框中，选择“无线网络配置”，在“首选网络”中选择“H3C-mac-vlan”，然后点击“属性”，如下图所示：

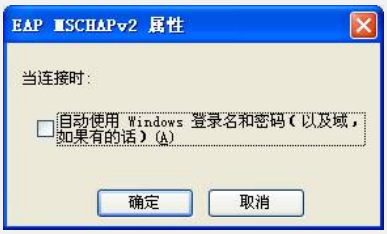
3、在弹出的“H3C-mac-vlan属性”对话框中，在“关联”项中根据SSID的配置，在“网络验证 (A)”中选择“WPA”，在“数据加密 (D)”中选择“TKIP”，如下图所示：

4、选择“验证”项，在“EAP类型 (T)”中选择“受保护的EAP (PEAP)”，然后点击“属性”，如下图所示：



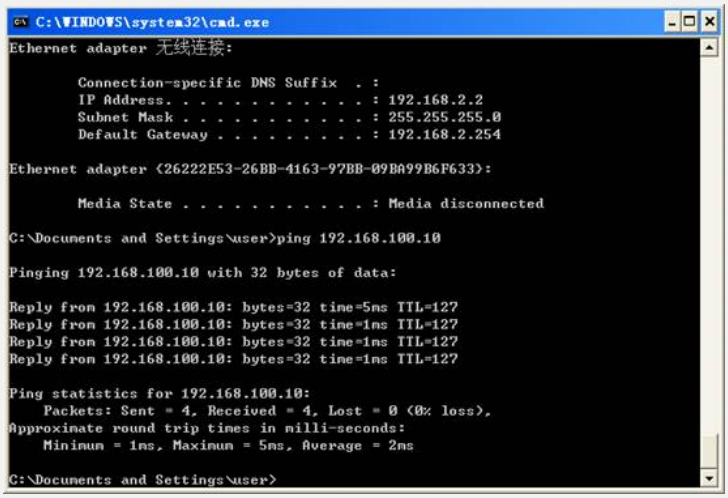
5、在弹出的“受保护的EAP属性”的对话框中，如需验证服务器证书，在“验证服务器证书 (V)”选项上打勾，否则勾掉该选项。然后点击“配置”，本例中不验证服务器证书，如下图所示：

6、在弹出的“EAP MSCHAPv2 属性”对话框中，勾掉“自动使用Windows登录名和密码”选项，然后选择“确定”。



七、验证结果

1、按照以上步骤完成客户端设置后，选择连接SSID H3C-mac-vlan，对弹出的对话框中输入用户名222和密码222，客户端属于VLAN 2，获取192.168.2.0/24网段地址，如下图所示：



2、选择连接SSID H3C-mac-vlan，对弹出的对话框中输入用户名333和密码333，客户端属于VLAN 3，获取192.168.3.0/24网段地址，如下图所示：