WA系列FAT AP动态VLAN下发功能的配置

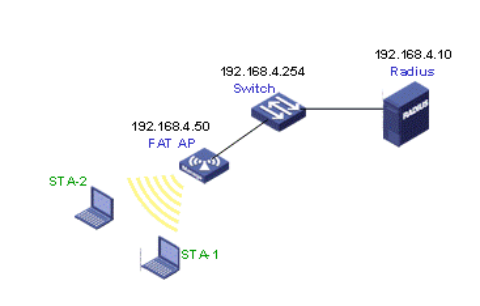
wlan接入 VLAN 宋斌 2011-08-09 发表

WA系列FAT AP动态VLAN下发功能的配置

一、 组网需求：

WA系列FAT AP（如WA2220-AG）、H3C PoE交换机、Radius服务器、便携机（安装有11b/g无线网卡）

二、 组网图：



FAT AP管理地址为192.168.4.50

Switch管理地址为192.168.4.254

Radius服务器管理地址为192.168.4.10，Radius服务器可采用H3C iMC管理软件或者CAMS软件，也可以采用Windows IAS组件。

三、 特性介绍：

基于MAC划分VLAN是VLAN的一种划分方法。它按照报文的源MAC地址来定义VLAN成员，将指定报文加入该VLAN的tag后发送。该功能通常会和安全（比如802.1X）技术联合使用，以实现终端的安全、灵活接入。

本特性提供了VLAN属性划分的另一种方法，并结合用户认证方法，确保安全合法用户获得VLAN权限，阻止非法用户于VLAN外，有效的起到了安全隔离及授权的作用。本特性的应用场合也比较灵活，适于需要进行VLAN受限分配的场合。

四、 配置信息：

```
#
 version 5.20, Release 1115
#
 sysname H3C
#
 domain default enable dot1x
#
 telnet server enable
#
 port-security enable
#
vlan 1
#
vlan 2 to 3
#
radius scheme dot1x
 primary authentication 192.168.4.10
 primary accounting 192.168.4.10
 key authentication h3c
 key accounting h3c
 user-name-format without-domain
#
domain dot1x
 authentication lan-access radius-scheme dot1x
 authorization lan-access radius-scheme dot1x
 accounting lan-access radius-scheme dot1x
```

```
 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
#
user-group system
#
local-user admin
 password simple h3capadmin
 authorization-attribute level 3
 service-type telnet
#
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 3 crypto
 ssid dot1x_mac_vlan
cipher-suite tkip
 security-ie wpa
 service-template enable
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.4.50 255.255.255.0
#
interface Ethernet1/0/1
port link-type trunk
port trunk permit vlan all
#
interface WLAN-BSS1
#
interface WLAN-BSS2
#
interface WLAN-BSS3
 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
#
interface WLAN-Radio1/0/1
#
interface WLAN-Radio1/0/2
 channel 1
 service-template 3 interface wlan-bss 3
#
 snmp-agent
 snmp-agent local-engineid 800063A203000FE207F2E0
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info version v3
#
 load xml-configuration
```

```
#
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
#
return
```

五、 主要配置步骤：

开启端口安全。

```
[H3C]port-security enable
```

配置无线接口，端口类型配置成hybrid口，并开启mac-vlan功能

```
[H3C]interface wlan-ess 3
[H3C-WLAN-ESS3] port link-type hybrid
[H3C-WLAN-ESS3] port hybrid vlan 1 to 3 untagged
[H3C-WLAN-ESS3] mac-vlan enable
[H3C-WLAN-ESS3] quit
```

配置接口采用802.1X认证方式。

```
[H3C-WLAN-ESS3] port-security port-mode userlogin-secure-ext
[H3C-WLAN-ESS3] port-security tx-key-type 11key
```

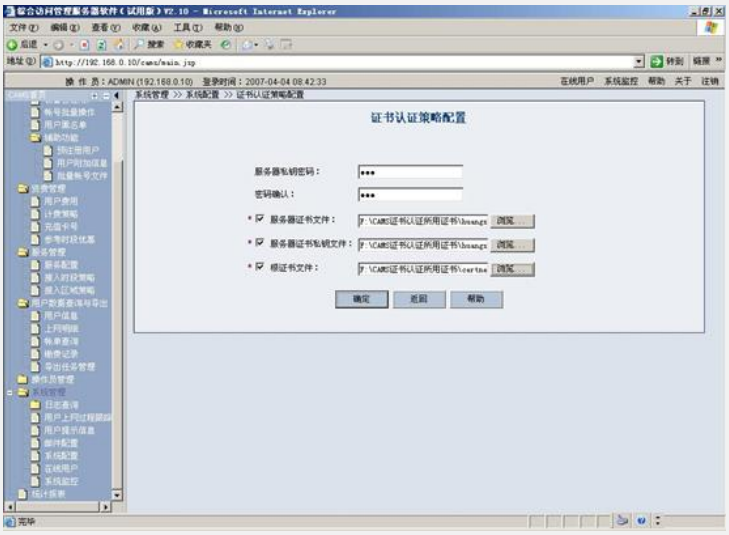
配置服务模板。

```
[H3C]wlan service-template 3 crypto
[H3C-wlan-st-3]ssid dot1x_mac_vlan
[H3C-wlan-st-3]bind wlan-ess 3
[H3C-wlan-st-3]cipher-suite tkip
[H3C-wlan-st-3]security-ie wpa
[H3C-wlan-st-3]service-template enable
[H3C-wlan-st-3]quit
```

配置Radius。这里首先介绍采用H3C CAMS进行配置的步骤操作：

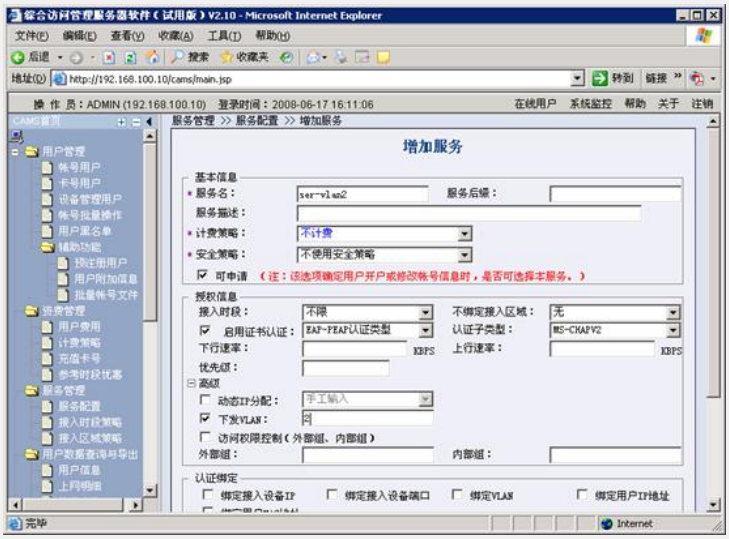
配置接入设备后再进行服务和用户名的配置

1、在CAMS系统的“系统管理>>系统配置>>证书认证策略配置”中进行如下图所示配置。



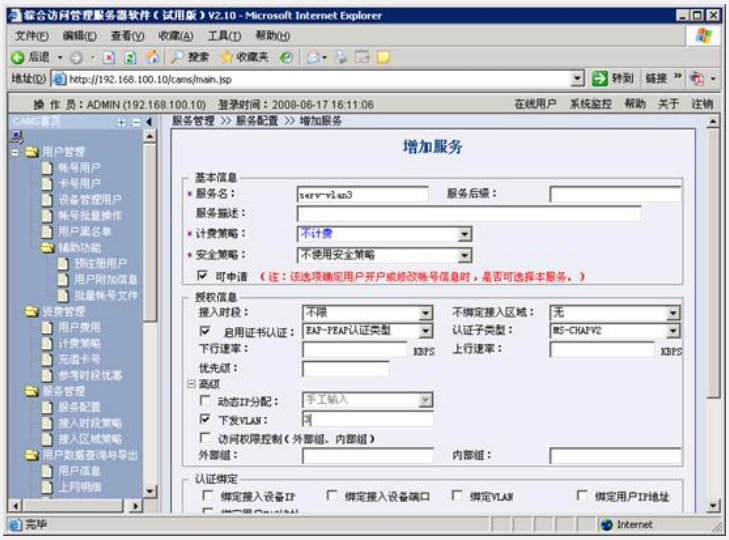
2、在CAMS系统的“服务管理>>服务配置>>增加服务”中进行如下图所示配置。增加服务名为“serv-vlan2”的服务，属性如下

- 启用证书认证为EAP-PEAP认证类型
- 认证子类型为MS-CHAPV2
- 高级->下发VLAN中填写“2”

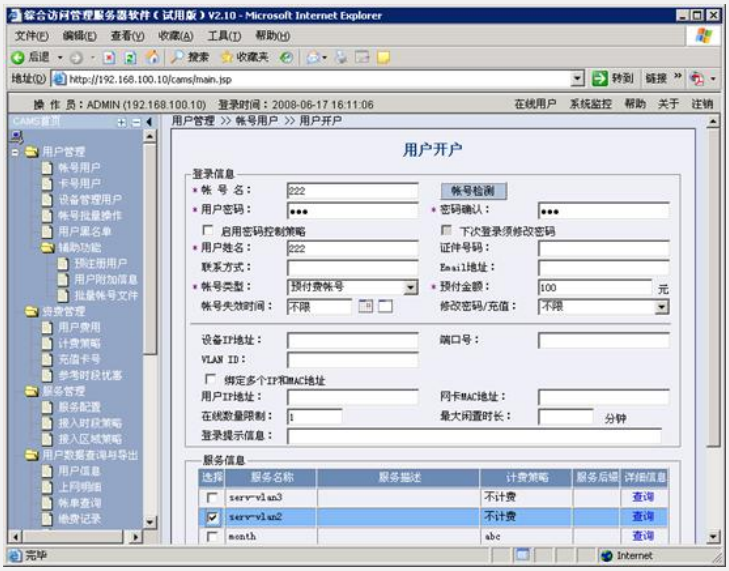


增加服务名为“serv-vlan3”的服务，属性如下

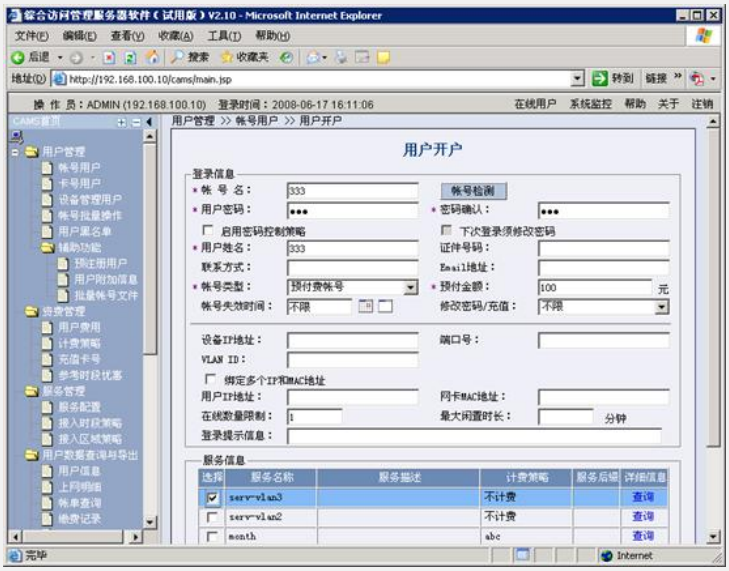
- 启用证书认证为EAP-PEAP认证类型
- 认证子类型为MS-CHAPV2
- 高级->下发VLAN中填写“3”



4、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。增加帐户名为“222”，密码为“222”，选择相应的服务“serv-vlan2”



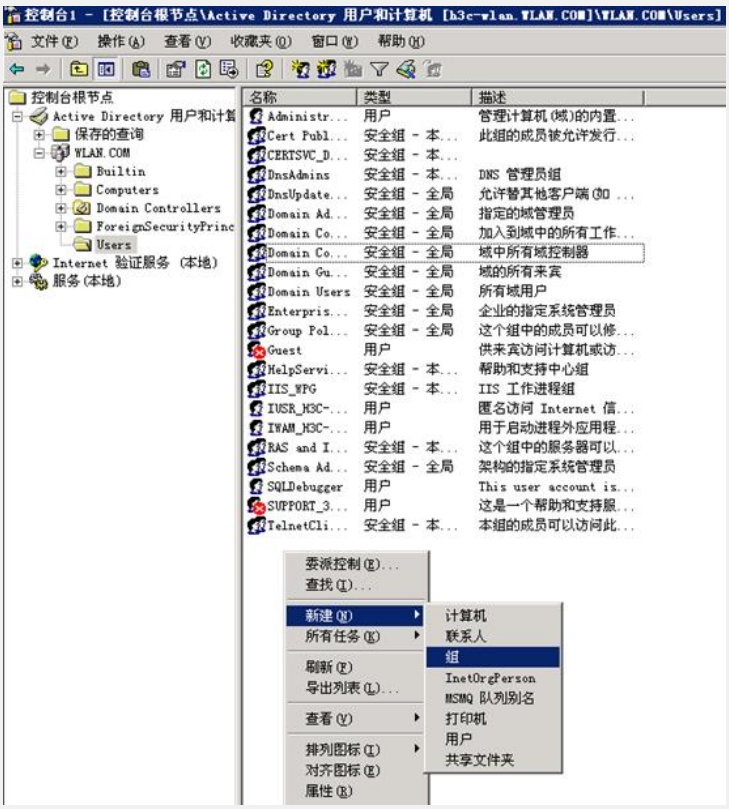
增加帐户名为“333”，密码为“333”，选择相应的服务“serv-vlan3”



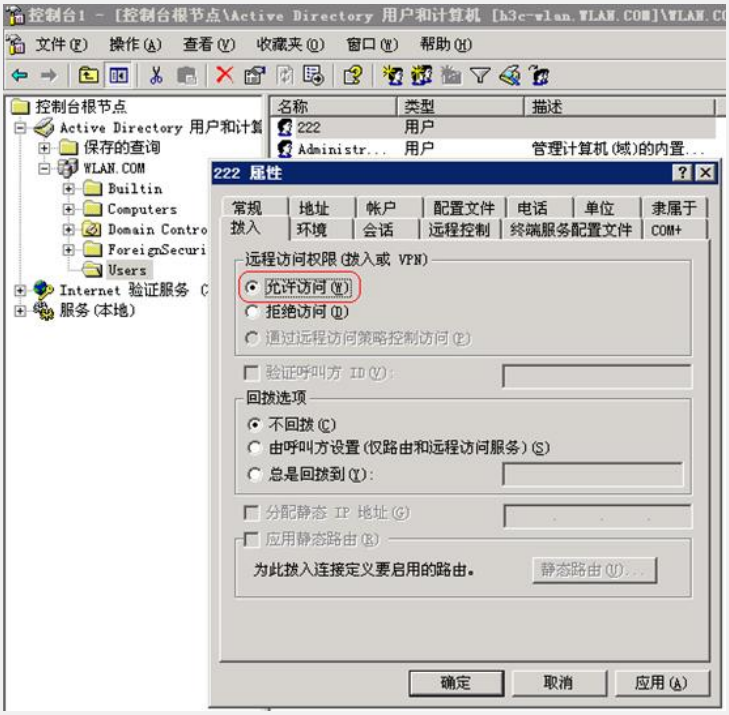
Radius也可以采用windows 的IAS组件：

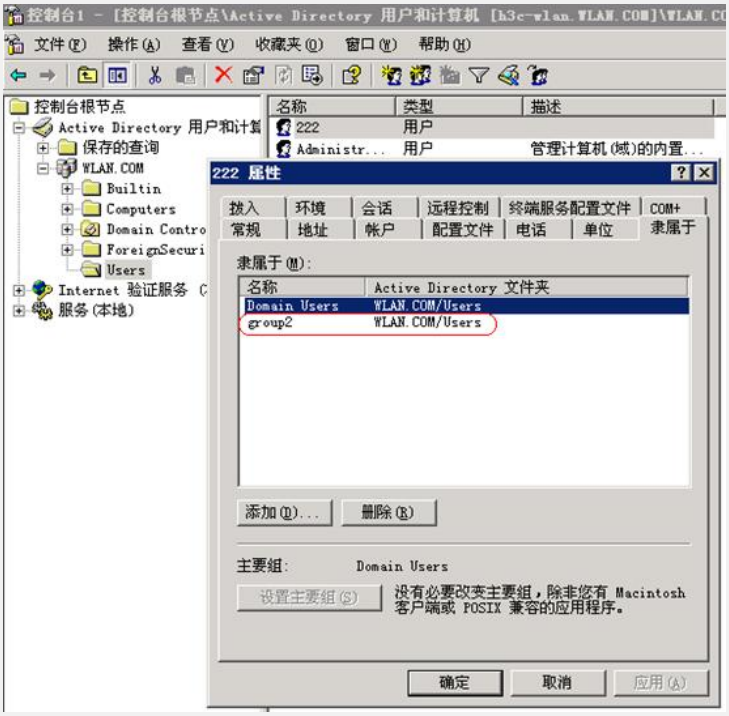
配置好Radius客户端后（Internet 验证服务），进行用户名和访问策略的配置：

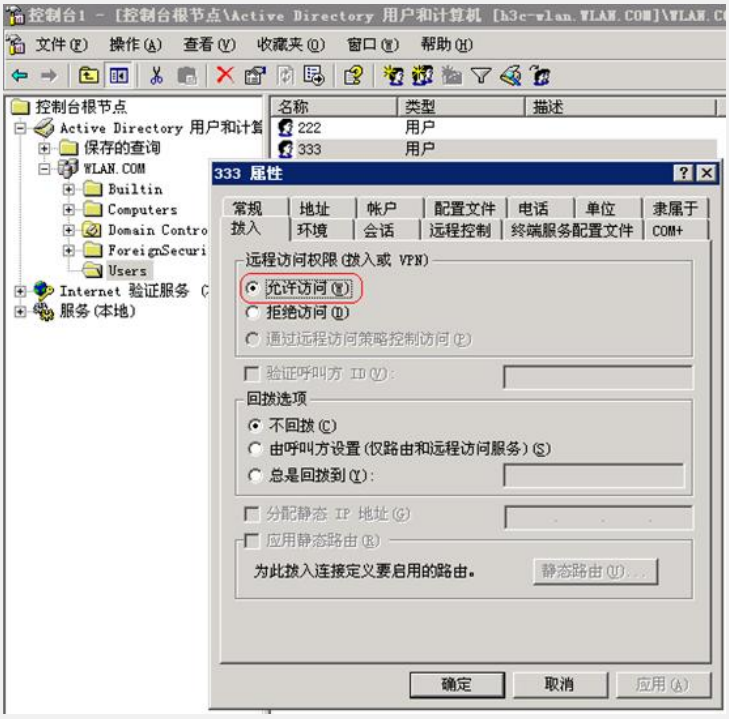
1、配置AD，增加两个用户组group2和group3

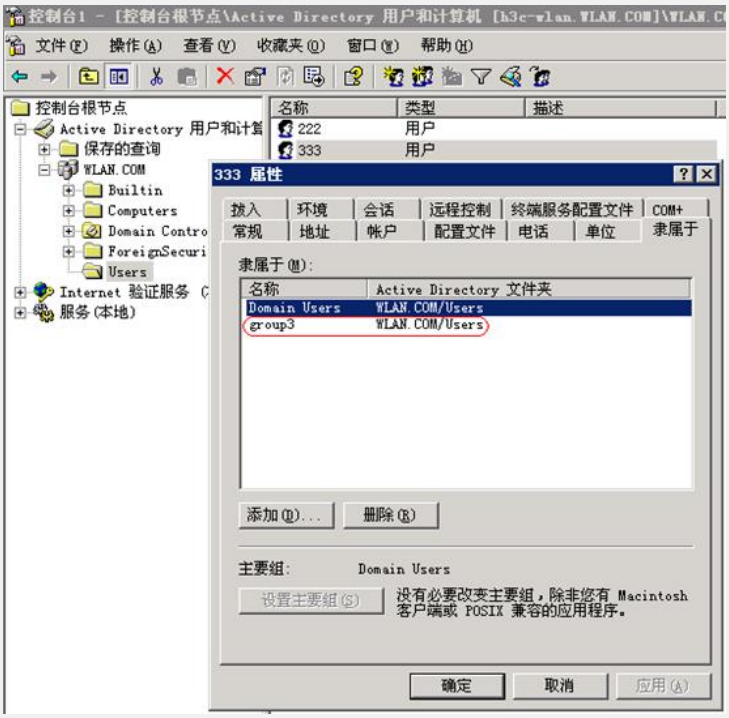


2、增加两个用户222和333，两个用户分别隶属于用户组group2和group3



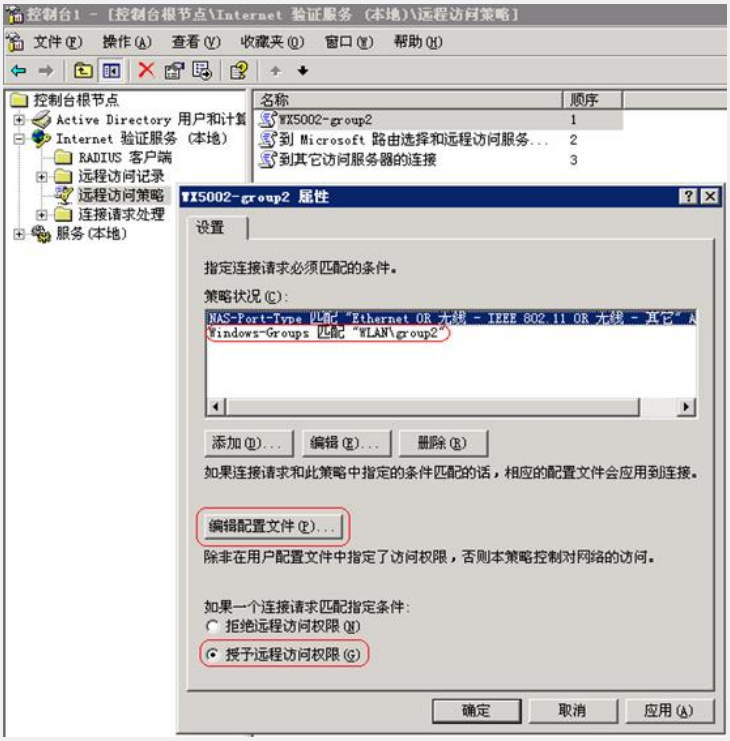




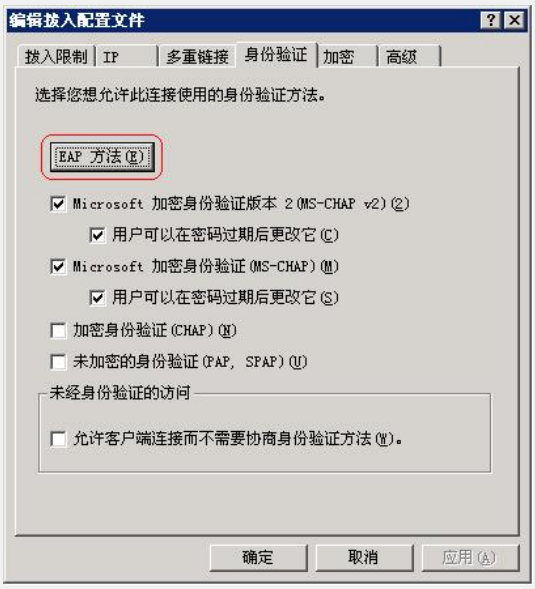


远程访问策略的相关配置

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：



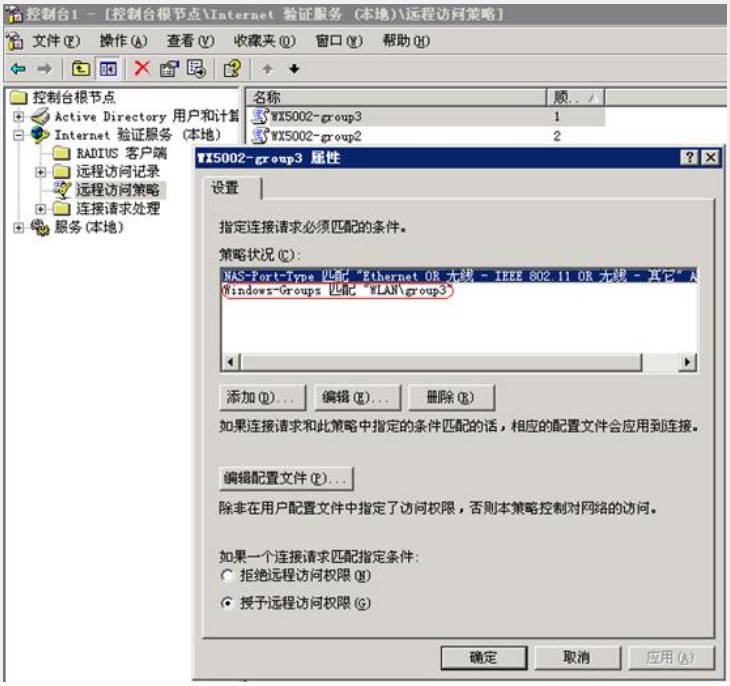
在“EAP方法”中选择“受保护的EAP（PEAP）”，如下图所示：

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、 结果验证：

当采用帐号“222”时，通过命令“display wlan client verbose”查看STA所属VLAN，如下：

```
[H3C] display wlan client verbose
 Total Number of Clients         : 1
 Total Number of Clients Connected : 1
                      Client Information
 ---------------------------------------------------------------
 MAC Address                  : 0012-f0cc-3a2c
 AID                          : 1
 Radio Interface              : WLAN-Radio1/0/2
 SSID                         : dot1x_mac_vlan
 BSSID                        : 000f-e250-22e0
 Port                         : WLAN-BSS3
 VLAN                         : 2
 State                        : Running
```

当采用帐号“333”时，通过命令“display wlan client verbose”查看STA所属VLAN，如下：

```
[H3C] display  wlan  client  verbose
 Total Number of Clients         : 1
 Total Number of Clients Connected : 1
                      Client Information
 ---------------------------------------------------------------
 MAC Address                  : 0012-f0cc-3a2c
 AID                          : 1
 Radio Interface              : WLAN-Radio1/0/2
 SSID                         : dot1x_mac_vlan
 BSSID                        : 000f-e250-22e0
 Port                         : WLAN-BSS3
 VLAN                         : 3
 State                        : Running
```