H3C 无线控制器

802.1X 远程认证典型配置举例(V7)

资料版本：6W100-20191125

目 录

1 简介

本文档介绍 802.1X 远程认证典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的无线控制器和接入点产品，不严格与具体硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 接入、WLAN 用户安全、WLAN 用户接入认证和 802.1X 的相关特性。

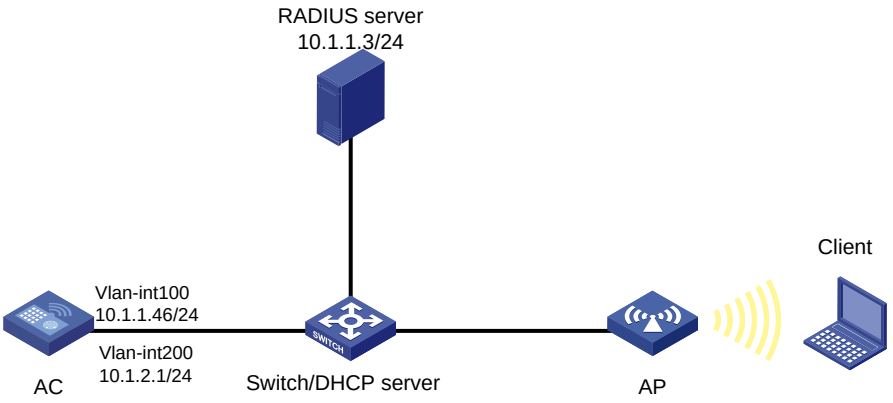
3 配置举例

3.1 组网需求

如图 1 所示组网，Switch 作为 DHCP server 为 AP 和 Client 分配 IP 地址，采用 iMC 作为 RADIUS 服务器对用户进行认证、授权和计费，要求：

- 对无线用户进行远程 802.1X 认证。
- 客户端链路层认证使用开放式系统认证。
- 通过配置客户端和 AP 之间的数据报文采用 802.1X 身份认证与密钥管理来确保用户数据的传输安全。
- 加密套件采用 CCMP。

图1 远程 802.1X 认证组网图



3.2 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

- 为了使服务器对用户授权信息进行动态修改或强制用户下线，必须开启 RADIUS session control 功能。
- 为了防止用户上线过程中，动态授权信息下发失败，需要配置 RADIUS DAE 服务器功能。

3.3 配置步骤

3.3.1 配置AC

(1) 配置 AC 的接口

创建 VLAN 100 以及对应的 VLAN 接口，并为该接口配置 IP 地址。AP 将获取该 IP 地址与 AC 建立 CAPWAP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.1.1.46 24
[AC-Vlan-interface100] quit
```

创建 VLAN 200 及其对应的 VLAN 接口，并为该接口配置 IP 地址。Client 将使用该 VLAN 接入无线网络。

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 10.1.2.1 24
[AC-Vlan-interface200] quit
```

(2) 配置 RADIUS 方案

创建 RADIUS 方案 radius1 并进入其视图。

```
[AC] radius scheme radius1
```

配置主认证/计费 RADIUS 服务器的 IP 地址为 10.1.1.3。

```
[AC-radius-radius1] primary authentication 10.1.1.3
[AC-radius-radius1] primary accounting 10.1.1.3
```

配置 AC 与认证/计费 RADIUS 服务器交互报文时的共享密钥为明文字符串 12345。

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

配置设备发送 RADIUS 报文使用的源 IP 地址为 10.1.2.1。

```
[AC-radius-radius1] nas-ip 10.1.2.1
[AC-radius-radius1] quit
```

创建名为 dom1 的 ISP 域并进入其视图。

```
[AC] domain dom1
```

配置 802.1X 用户使用 RADIUS 方案 radius1 进行认证、授权、计费。

```
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

使能 RADUIS session control 功能。

```
[AC] radius session-control enable
```

开启 RADIUS DAE 服务，并进入 RADIUS DAE 服务器视图。

```
[AC] radius dynamic-author server
```

设置 RADIUS DAE 客户端的 IP 地址为 10.1.1.3，与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥为明文 12345。

```
[AC-radius-da-server] client ip 10.1.1.3 key simple 12345
[AC-radius-da-server] quit
```

(3) 配置 802.1X 认证

配置 802.1X 系统的认证方法为 EAP。

```
[AC] dot1x authentication-method eap
```

(4) 配置无线服务模板

创建无线服务模板 service，并进入无线服务模板视图。

```
[AC] wlan service-template service
```

配置 SSID 为 service。

```
[AC-wlan-st-service] ssid service
```

配置无线服务模板 VLAN 为 200。

```
[AC-wlan-st-service] vlan 200
```

配置身份认证与密钥管理的模式为 802.1X。

```
[AC-wlan-st-service] akm mode dot1x
```

配置 CCMP 为加密套件，配 RSN 为安全信息元素。

```
[AC-wlan-st-service] cipher-suite ccmp
[AC-wlan-st-service] security-ie rsn
```

配置用户接入认证模式为 802.1X。

```
[AC-wlan-st-service] client-security authentication-mode dot1x
```

配置 802.1X 用户使用认证域为 dom1。

```
[AC-wlan-st-service] dot1x domain dom1
```

使能无线服务模板。

```
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

创建 AP，配置 AP 名称为 office，型号名称选择 WA4320i-ACN，并配置序列号 210235A1GQC158004457。

```
[AC] wlan ap office model WA4320i-ACN
[AC-wlan-ap-office] serial-id 210235A1GQC158004457
```

进入 Radio 1 视图。

```
[AC-wlan-ap-office] radio 1
```

将无线服务模板 service 绑定到 radio 1，并开启射频。

```
[AC-wlan-ap-office-radio-1] service-template service
[AC-wlan-ap-office-radio-1] radio enable
[AC-wlan-ap-office-radio-1] quit
[AC-wlan-ap-office] quit
```

3.3.2 配置Switch

创建 VLAN 100，用于转发 AC 和 AP 间 CAPWAP 隧道内的流量。

```
<Switch> system-view
```

```
[Switch] vlan 100
[Switch-vlan100] quit
```
创建 VLAN 200，用于转发 Client 无线报文。
```
[Switch] vlan 200
[Switch-vlan200] quit
```
配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，允许 VLAN 100 和 VLAN 200 通过。
```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```
配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。
```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```
使能 PoE 功能。
```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```
配置 VLAN 100 接口的 IP 地址。
```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 10.1.1.47 24
[Switch-Vlan-interface100] quit
```
配置 VLAN 200 接口的 IP 地址。
```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 10.1.2.2 24
[Switch-Vlan-interface200] quit
```
配置 DHCP 地址池 100，用于为 AP 分配 IP 地址。
```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 10.1.1.0 mask 255.255.255.0
[Switch-dhcp-pool-100] gateway-list 10.1.1.46
[Switch-dhcp-pool-100] quit
```
配置 DHCP 地址池 200，用于为 Client 分配 IP 地址，为 Client 分配的 DNS 服务器地址为网关地址（实际使用过程中请根据实际网络规划配置无线客户端的 DNS 服务器地址）。
```
[Switch] dhcp server ip-pool 200
[Switch-dhcp-pool-200] network 10.1.2.0 mask 255.255.255.0
[Switch-dhcp-pool-200] gateway-list 10.1.2.1
[Switch-dhcp-pool-200] dns-list 10.1.2.1
[Switch-dhcp-pool-200] quit
```
开启 DHCP 服务。
```
[Switch] dhcp enable
```

3.3.3 配置RADIUS server

说明

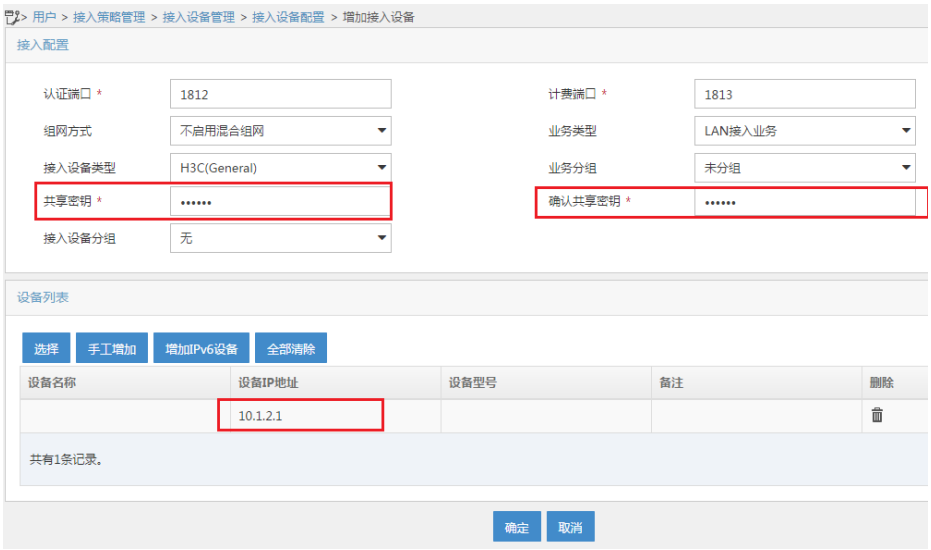
下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.1(E0302)、iMC UAM 7.1(E0302)），说明 AAA 服务器的基本配置。

增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入配置管理页面。在该页面中点击<增加>按钮，进入增加接入设备页面。

- 设置认证、计费共享密钥为 12345，其它保持缺省配置；
- 选择或手工增加接入设备，添加 IP 地址为 10.1.2.1 的接入设备。

图2 增加接入设备页面

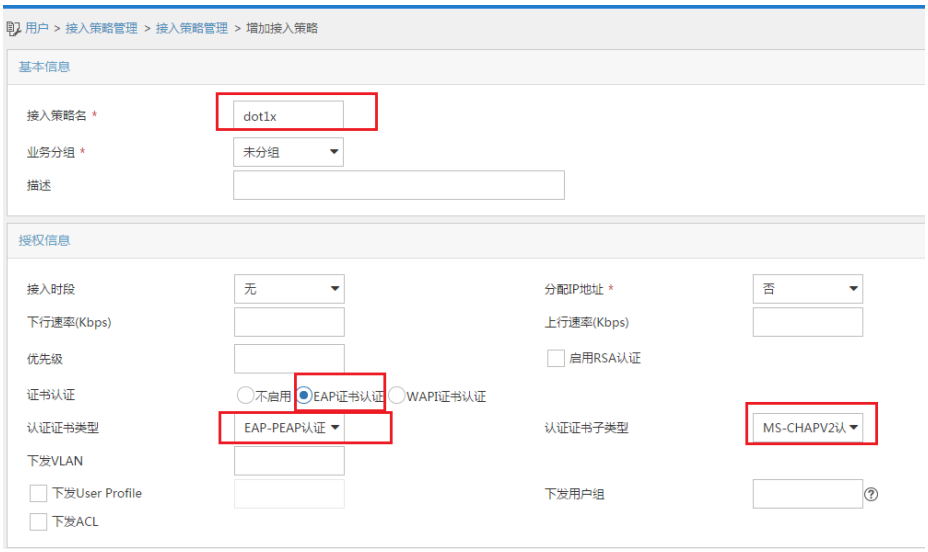


增加接入策略。

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略管理页面，在该页面中单击<增加>按钮，进入增加接入策略页面。

- 设置接入策略名输入 dot1x；
- 选择证书认证为 EAP 证书认证；
- 选择认证证书类型为 EAP-PEAP 认证，认证证书子类型为 MS-CHAPV2 认证。认证证书子类型需要与客户端的身份验证方法一致。

图3 增加服务策略页面

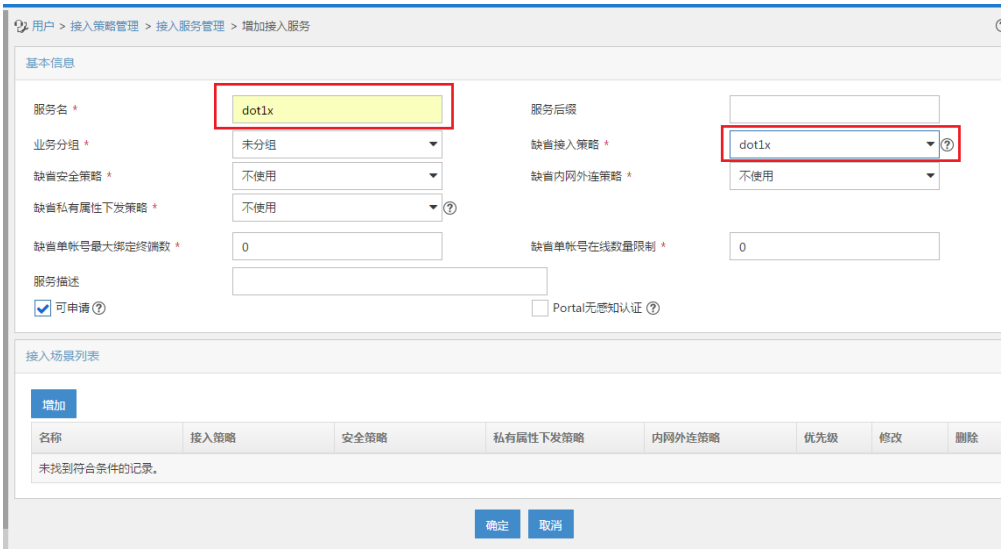


增加接入服务。

选择“用户”页签，单击导航树[接入策略管理/接入服务管理]菜单项，进入接入服务管理页面，在该页面中单击<增加>按钮，进入增加接入服务页面。

- 设置服务名为 dot1x；
- 设置缺省接入策略为已经创建的 dot1x 策略。

图4 增加接入服务页面

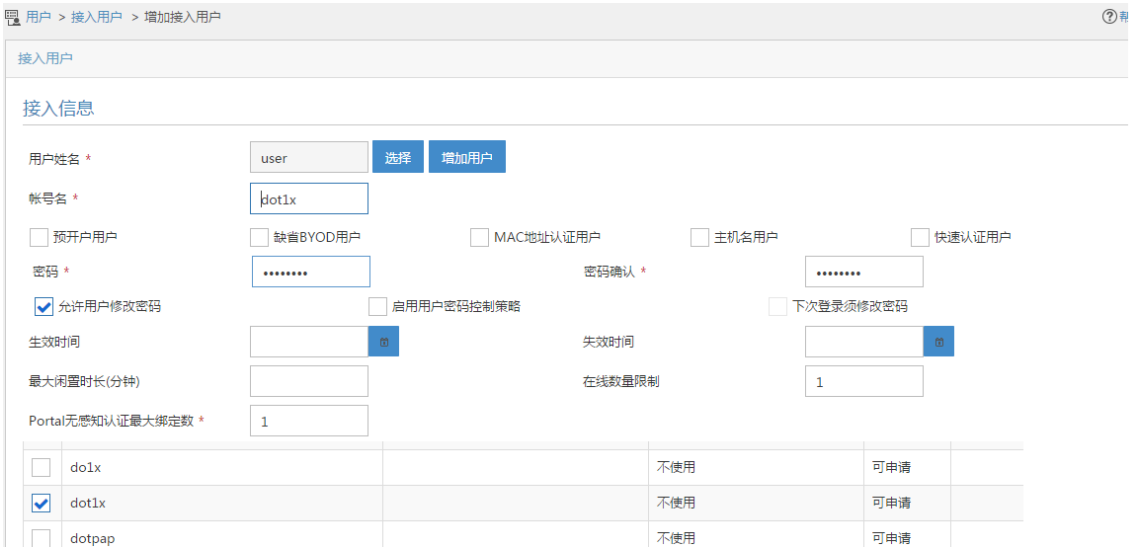


增加接入用户。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 添加用户 user；
- 添加账号名为 dot1x，密码为 dot1x123；
- 选中之前配置的服务 dot1x。

图5 增加接入用户页面



3.3.4 配置客户端

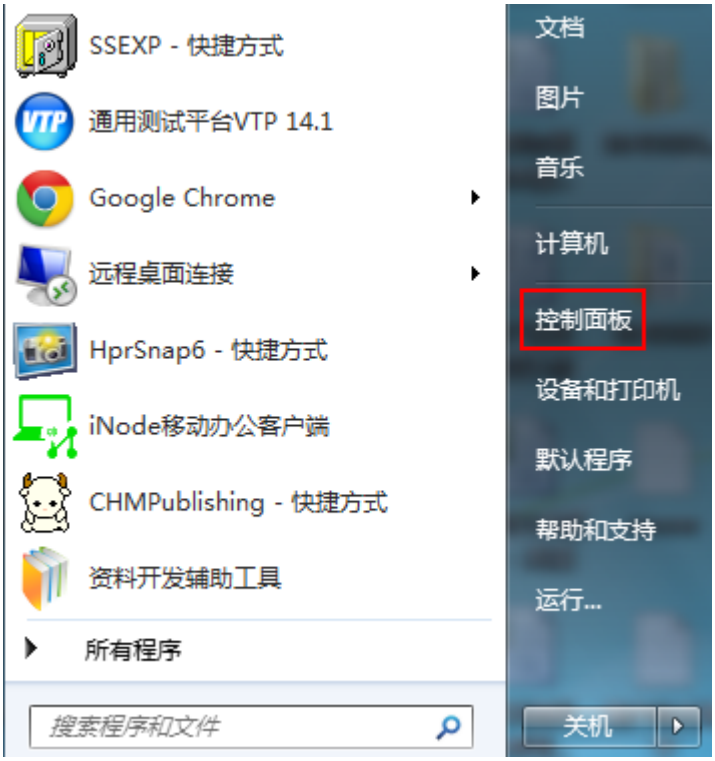
配置无线网卡

说明

- 下面以 Windows 7 Service Pack 1 为例，说明无线网卡的配置。
- 在客户端上已经完成证书安装。

打开“开始”菜单，单击“控制面板”，进入控制面板窗口。

图6 打开控制面板



单击“查看网络状态和任务”，进入到了“网络和共享中心”。

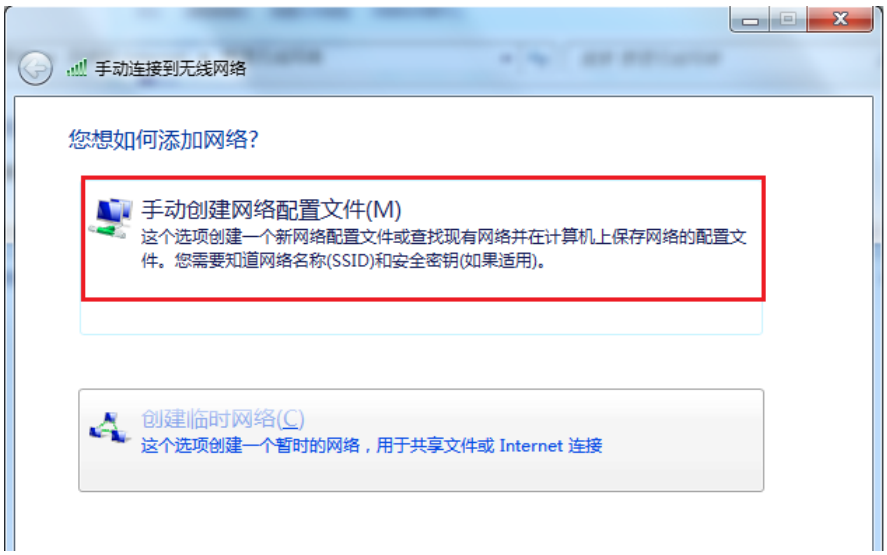
图7 查看网络状态和任务

单击“管理无线网络”，进入管理无线网络窗口。

图8 管理无线网络

单击<添加>按钮，选择“手动创建网络配置文件(M)”。

图9 手动添加无线网络



添加无线网络信息。

- 输入网络名(服务模板中的 ssid):service；
- 选择安全类型:WPA2-企业；
- 加密类型：AES；
- 其它保持缺省配置，然后单击“下一步”。

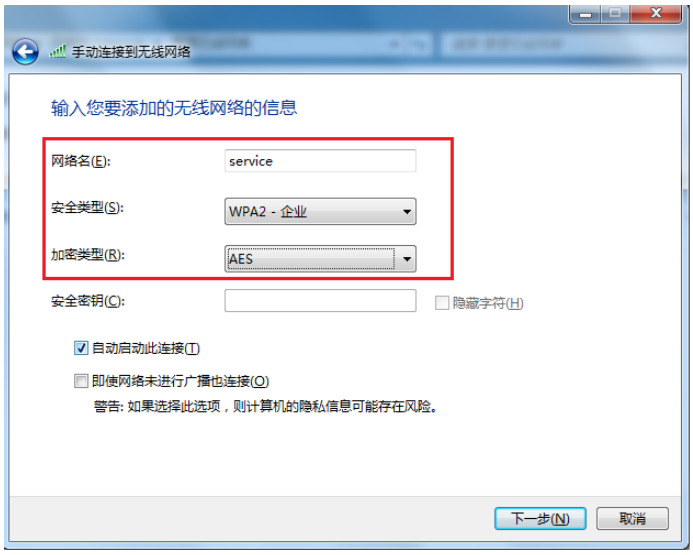
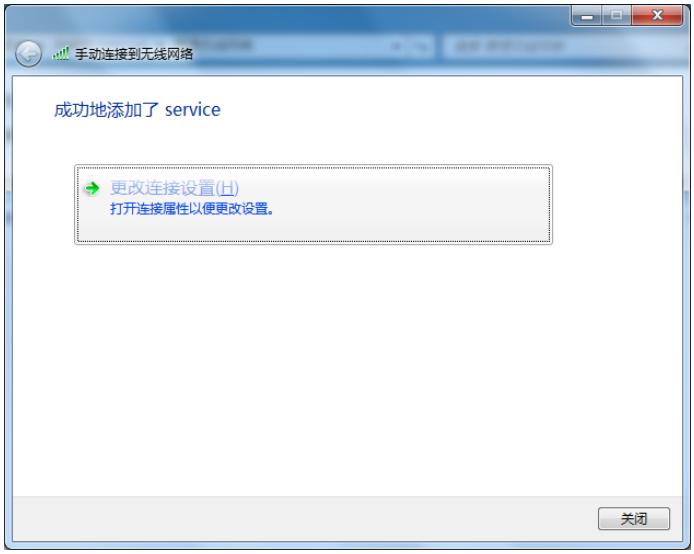
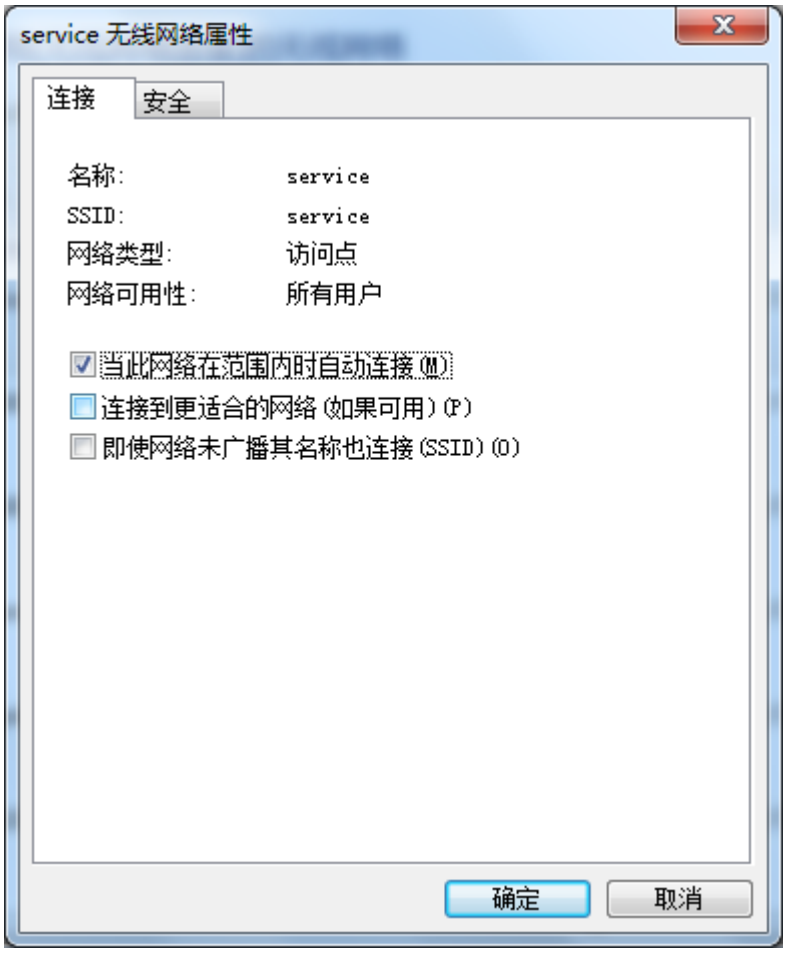


图10 无线网络创建成功



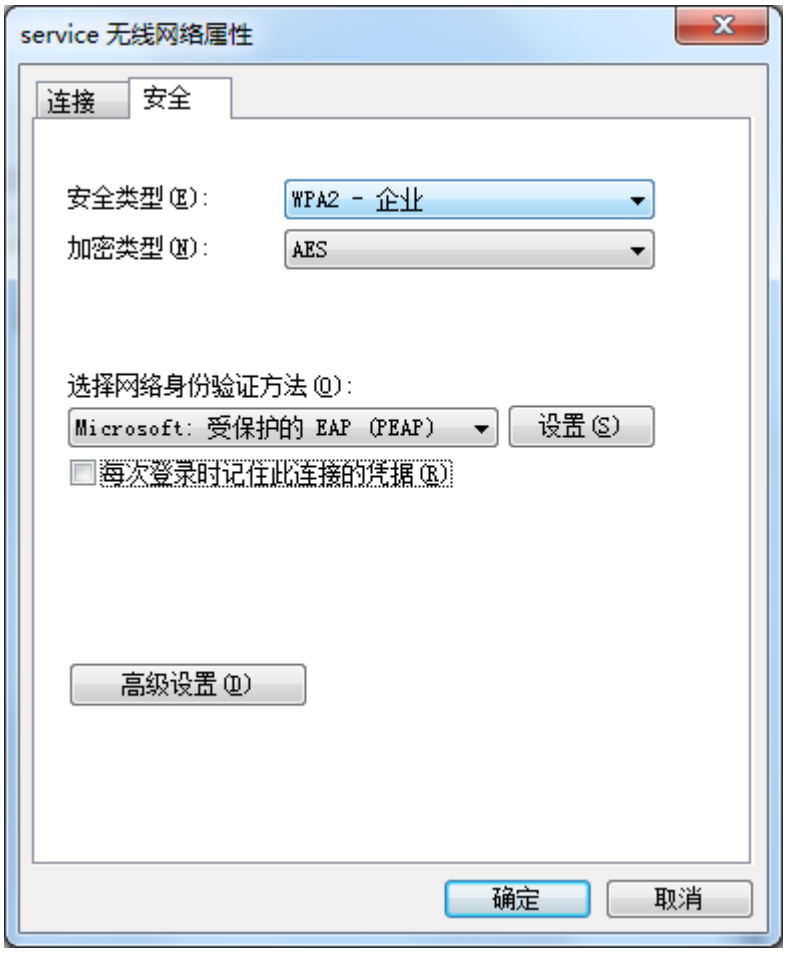
网络创建成功后，选择“更改连接设置(H)”，进入无线网络属性对话框。

图11 无线网络属性



单击“安全”页签，在“选择网络身份验证方法”下拉框中选择“Microsoft:受保护的 EAP（PEAP）”，然后将 “每次登录时记住此连接的凭据” 前的复选框中的勾去掉。

图12 网络身份验证配置



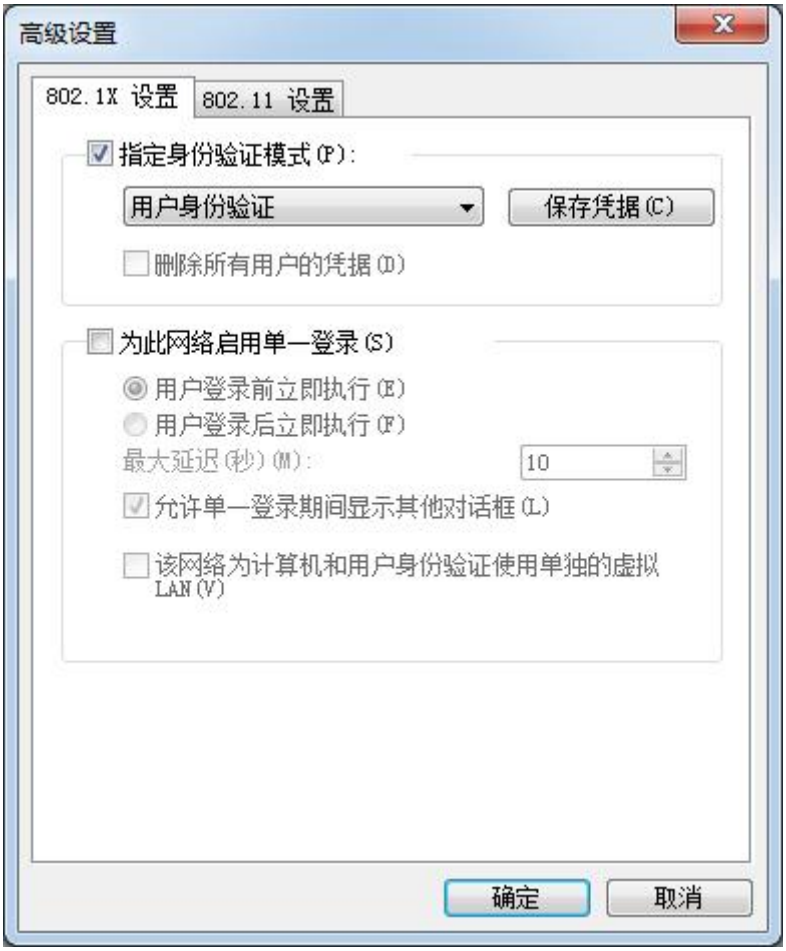
单击<设置>按钮，进入“保护的 EAP 属性”对话框。

- 去掉“验证服务器证书(V)”前复选框中的勾；
- 去掉“启用快速重新连接”前复选框中的勾；
- 单击“选择身份验证方法(S)”后面的<配置>按钮；
- 在弹出的“EAP MSCHAPv2 属性”对话框中，去掉复选框中的勾；
- 然后单击<确定>按钮，返回“受保护的 EAP 属性”界面，再单击<确定>按钮。

图13 属性配置

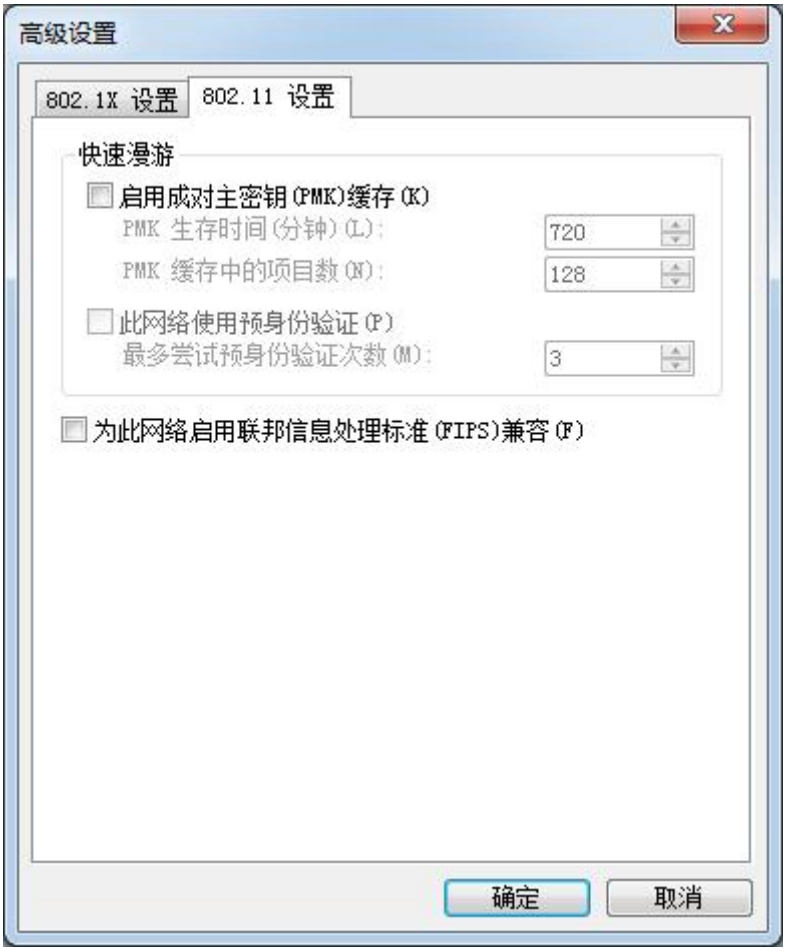
在无线网络属性对话框中，单击<高级设置>按钮，进入高级设置对话框。在 802.1X 设置页签中，勾选“指定身份验证模式”，然后，在下拉框中选择“用户身份验证”。

图14 高级设置-802.1X 设置



单击“802.11 设置”页签，去掉“启用成对主密钥(PMK)缓存”前的复选框中的勾，然后单击<确定>按钮。

图15 无线网卡配置过程



3.4 验证配置

客户端通过 802.1X 认证成功关联 AP，并且可以访问无线网络。

在 AC 上可以通过 **display wlan client verbose** 命令查看客户端上线情况。

```
[AC] display wlan client verbose
Total number of clients: 1

 MAC address                          : cc3a-61a8-fb8c
 IPv4 address                         : 10.1.2.3
 IPv6 address                         : N/A
 Username                             : user
 AID                                  : 1
 AP ID                                : 3
 AP name                              : office
 Radio ID                             : 1
 SSID                                 : service
 BSSID                                : 741f-4ad4-1fe0
 VLAN ID                              : 200
```

```
 Sleep count                          : 0
 Wireless mode                        : 802.11ac
 Channel bandwidth                    : 80MHz
 SM power save                        : Disabled
 Short GI for 20MHz                   : Supported
 Short GI for 40MHz                   : Supported
 Short GI for 80MHz                   : Supported
 Short GI for 160/80+80MHz            : Not supported
 STBC RX capability                   : Not supported
 STBC TX capability                   : Not supported
 LDPC RX capability                   : Not supported
 SU beamformee capability             : Not supported
 MU beamformee capability             : Not supported
 Beamformee STS capability            : N/A
 Block Ack                            : N/A
 Supported VHT-MCS set                : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
 Supported HT MCS set                 : 0, 1, 2, 3, 4, 5, 6, 7
 Supported rates                      : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
 QoS mode                             : WMM
 Listen interval                      : 10
 RSSI                                 : 0
 Rx/Tx rate                           : 0/0
 Authentication method                : Open system
 Security mode                        : RSN
 AKM mode                             : 802.1X
 Cipher suite                         : CCMP
 User authentication mode             : 802.1X
 Authorization ACL ID                 : N/A
 Authorization user profile           : N/A
 Roam status                          : N/A
 Key derivation                       : SHA1
 PMF status                           : N/A
 Forwarding policy name               : N/A
 Online time                          : 0days 0hours 0minutes 15seconds
 FT status                            : Inactive
```

在 AC 上可以通过 **display dot1x connection** 命令查看 dot1x 用户上线情况。

```
[AC] display dot1x connection
Total connections: 1

User MAC address           : cc3a-61a8-fb8c
AP name                    : office
Radio ID                   : 1
SSID                       : service
BSSID                      : 741f-4ad4-1fe0
Username                   : user
Authentication domain      : dom1
IPv4 address               : 10.1.2.3
Authentication method      : EAP
```

```
Initial VLAN               : 200
Authorization VLAN         : 200
Authorization ACL number   : N/A
Authorization user profile : N/A
Termination action         : Default
Session timeout period     : 36000001 s
Online from                : 2015/12/21 11:27:11
Online duration            : 0h 1m 1s
```

3.5 配置文件

- AC：

```
#
 dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
wlan service-template service
 ssid service
vlan 200
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain dom1
 service-template enable
#
interface Vlan-interface100
 ip address 10.1.1.46 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.1 255.255.255.0
#
radius scheme radius1
 primary authentication 10.1.1.3
 primary accounting 10.1.1.3
 key authentication cipher $c$3$Bb61SHV2ZsVYPJU2+RFB/8ntk0uCQkmxdA==
 key accounting cipher $c$3$w03NfxnBmfDuedv9/xo7ESnoxKjowmmX9A==
nas-ip 10.1.2.1
#
radius dynamic-author server
 client ip 10.1.1.3 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dom1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
```

```
 accounting lan-access radius-scheme radius1
#
wlan ap office model WA4320i-ACN
 serial-id 210235A1GQC158004457
 radio 1
  radio enable
    service-template service
#
```

- Switch：

```
#
 dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
 gateway-list 10.1.1.46
 network 10.1.1.0 mask 255.255.255.0
#
dhcp server ip-pool 200
 gateway-list 10.1.2.1
 network 10.1.2.0 mask 255.255.255.0
 dns-list 10.1.2.1
#
interface Vlan-interface100
 ip address 10.1.1.47 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 100
 poe enable
#
```

4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“用户接入与认证配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“用户接入与认证命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 接入配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 接入命令参考”。