WX系列AC 远程802.1X无线认证和IMCv7配合典型配置案例及认证过程分析

802.1X wlan接入 AAA 吴骋骐 2014-04-16 发表

WX系列AC 远程802.1X无线认证和IMCv7配合典型配置案例及认证过程分析

一、组网需求及背景

1.802.1x认证介绍

802.1x协议通俗意义上是一个通用认证的封装协议，可以封装多种认证，对于WLAN网络比较常用的有PEAP和EAP-TLS，而PAP和CHAP不能使用，因为在WLAN网络中802.1x认证过程还有一个重要的作用就是在客户端和设备侧协商产生一个4-way handshake协商的种子密钥，而PAP和CHAP是无法完成该功能的。

802.1x协议主要实现认证设备和认证终端之间的交互，而对具体的认证报文会通过radius发送给认证服务器。设备首先请求客户端的ID来触发802.1x认证，之后实际上实现了802.1x报文和radius报文之间的一个中继功能，将来自无线客户端的802.1x报文的认证信息进行中继通过radius报文发送给指定的认证服务器；同时将认证服务器回应的radius报文解析转换成802.1x报文并最终发送给无线客户端。

对于802.1x认证本身，无线用户和有线用户没有任何的差别，只是无线用户在认证成功后会使用认证过程中产生的radius key生成后续4-way handshake的种子密钥。

另外，顺带说明4-way handshake可以作为802.1x协议的一部分，是专门为WLAN设计，通过802.1x的EAPOL-Key报文完成无线客户端和设备之间的密钥协商。WPA2+PSK还是WPA2+802.1x接入都存在4-way handshake过程协商无线链路的密钥，唯一的区别使用PSK方式的时候前面没有任何的其他认证，而是在4-Way handshake过程中同步完成PSK认证。

2.认证流程说明：

1.在整个过程之前，还有一个WLAN服务的通告或者搜索过程：AP定期主动的发送Beacon报文通告可以提供的WLAN服务；无线客户端可以发送Probe request报文搜索周围的WLAN无线网络；

2.Open-system Authentication过程和Association过程就是802.11链路的协商过程，无论接入哪种WLAN服务都必须通过这两个过程先建立802.11的无线链路，之后在无线链路建立成功的基础上，才可以完成其他的业务，例如密钥协商、地址申请、访问网络，等等；

3.从“EAPOL Start”到“认证成功”整个过程为802.1x认证过程，整个过程可能有多个报文交互，而且随着使用的EAP认证方式不同，报文的交互有所不同。当802.1x认证成功后，802.1x客户端和Radius server会产生一个相同的Radius key，该Radius key将会生成后面密钥协商的PMK；

4.“4次握手Key协商”过程就是通常提到的密钥协商过程，该过程使用802.1x认证产生的PMK作为种子密钥，在无线客户端和AP之间动态协商出后续无线链路传输数据报文所要使用的各种密钥；

5.当上面的所有过程完成后，该无线客户端才会认为成功接入到WLAN服务中；如果任何一个环节出现错误都会被认为无线结果失败，AP会主动发送Disassociation报文将该无线客户端断开；

3.802.1x协商过程介绍

802.1x协议实际上在WLAN网络上才真正得到全面的应用，而过去有线网络的802.1x认证只是使用了802.1x的认证部分的功能。

802.1x协议从功能上可以分为两大部分：认证部分和密钥协商部分。其中，认证部分需要客户端、设备和认证服务器共同参与，最终完成对客户端的接入认证，特别在WLAN协议中还会在客户端和认证服务器（包括设备）端协商一个radius key，带密钥将被作为后续密钥协商的种子密钥。而密钥协商部分（4-way handshake）只是在设备和客户端之间进行交互，完成对称密钥的协商和生成，生成的密钥最终会作为802.11链路使用的系列密钥。

下面介绍一下802.1x协商过程中的几个关键报文:

认证开始报文：1、客户端发送EAP-Start报文触发认证；2、设备侧会发送EAP request报文请求客户端的用户名信息，启动对客户端的认证。

认证成功报文：当所有的认证成功以后，设备会向客户端发送EAP-Success报文通知客户端认证成功。协议认为该报文作为消息通知报文，不需要进行重传。

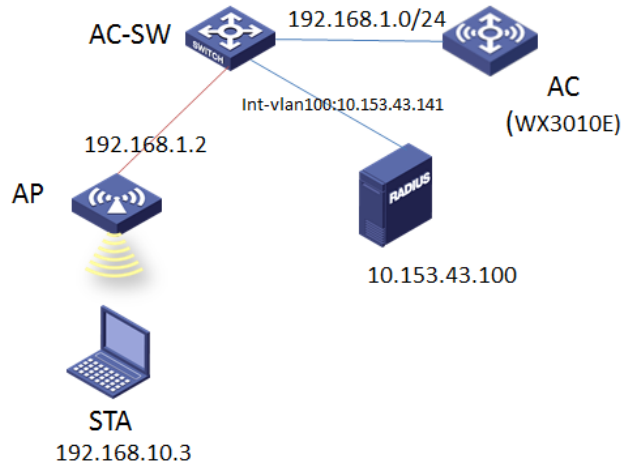
认证下线或者失败报文：客户端也可以发送EAPOL-Logoff报文给设备端，主动要求下线。设备端把端口状态从授权状态改变成未授权状态，并向客户端发送EAP-Failure报文

密钥协商报文：EAPOL-Key报文，目前仅支持802.11Key方式的密钥协商，可以包括两个协

商过程（4-way handshake和Group Key handshake）。目前该部分功能在WLAN的MAC模块完成，但是报文收发由802.1x模块完成。

根据目前的经验整个802.1x认证过程的协商报文可能超过20多个报文，在这个过程任何的一个报文出现丢失，都需要802.1x协议重传机制进行适当的保护，而这个重传机制直接决定了此次协商所需要的时间。

4.组网需求



本配置举例中，使用WX3010E作为无线控制器，版本号为R3507P14。AC作为AP网关（vlan-interface10:192.168.1.1/24）并配置DHCP server为AP分配IP地址。AC作为STA网关(vlan-interface10：192.168.10.1/24)并配置DHCP Server为STA分配IP地址。交换机为AP提供POE供电。

二、配置步骤

1、AC侧配置

```
[WX3010E]dis cu
#
 version 5.20, Release 3507P14
#
 sysname WX3010E
#
 configure-user count 6
#
 domain default enable dot1x
#
 telnet server enable
#
 port-security enable
#
 dot1x authentication-method eap
#
 oap management-ip 192.168.0.101 slot 0
#
 password-recovery enable
#
 vlan 1
```

```
#
vlan 10
#
vlan 100
#
radius scheme imc
 server-type extended
 primary authentication 10.153.43.100
 primary accounting 10.153.43.100
 key authentication cipher $c$3$AIgC2dNmRlbCWNjuhqz3Z5aCVeu6iA==
 key accounting cipher $c$3$o1Oiwu5dwthrUwlzdk02tCtcTobSMg==
 user-name-format without-domain
 nas-ip 10.153.43.141
#
domain dot1x
 authentication lan-access radius-scheme imc
 authorization lan-access radius-scheme imc
 accounting lan-access radius-scheme imc
 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 ap
 network 192.168.1.0 mask 255.255.255.0
 gateway-list 192.168.1.1
#
dhcp server ip-pool sta
 network 192.168.10.0 mask 255.255.255.0
 gateway-list 192.168.10.1
 dns-list 9.9.9.9
#
user-group system
 group-attribute allow-guest
#
local-user admin
 password cipher $c$3$VnWjDhTHgrxykrRnOJv3ANrCmwfBPzB9
 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 1 crypto
 ssid h3c-1x
 bind WLAN-ESS 1
 cipher-suite tkip
 security-ie wpa
 service-template enable
#
wlan ap-group default_group
 ap ap1
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface10
 ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface100
 ip address 10.153.43.141 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
interface WLAN-ESS1
 port access vlan 10
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
 dot1x mandatory-domain dot1x
```

```
#
wlan ap ap1 model WA2620 id 1
 serial-id 5866-BA5E-C6E0
 radio 1
 radio 2
  channel 6
  max-power 15
  service-template 1
  radio enable
#
snmp-agent
 snmp-agent local-engineid 800063A203000FE2873066
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 10.153.43.100 params securityname pu
blic v2c
#
wlan ips
 malformed-detect-policy default
 signature deauth_flood signature-id 1
 signature broadcast_deauth_flood signature-id 2
 signature disassoc_flood signature-id 3
 signature broadcast_disassoc_flood signature-id 4
 signature eapol_logoff_flood signature-id 5
 signature eap_success_flood signature-id 6
 signature eap_failure_flood signature-id 7
 signature pspoll_flood signature-id 8
 signature cts_flood signature-id 9
 signature rts_flood signature-id 10
 signature-policy default
 countermeasure-policy default
 attack-detect-policy default
 virtual-security-domain default
  attack-detect-policy default
  malformed-detect-policy default
  signature-policy default
  countermeasure-policy default
#
 dhcp enable
#
 arp-snooping enable
#
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
```

#

Return

主要配置步骤

(1)创建radius方案

#创建radius方案imc并进入其视图

[WX3010E]radius scheme imc

#radius服务器类型设置为extended

[WX3010E-radius-imc]server-type extended

#配置主认证radius服务器的ip地址

[WX3010E-radius-imc]primary authentication 10.153.43.100

#配置主计费radius服务器的ip地址

[WX3010E-radius-imc]primary accounting 10.153.43.100

设置系统与认证RADIUS服务器交互报文时的共享密钥为h3c。

[WX3010E-radius-imc]key authentication h3c

设置系统与计费RADIUS服务器交互报文时的共享密钥为h3c。

[WX3010E-radius-imc]key accounting h3c

#绑定nas-ip

[WX3010E-radius-imc]nas-ip 10.153.43.141

(2)创建domain域

创建dot1x域并进入其视图

[WX3010E]domain dot1x

#为lan-access用户配置认证方案为RADIUS方案，方案名为imc

[WX3010E-isp-dot1x]authentication lan-access radius-scheme imc

#为lan-access用户配置授权方案为RADIUS方案，方案名为imc

[WX3010E-isp-dot1x]authorization lan-access radius-scheme imc

#为lan-access用户配置计费方案为RADIUS方案，方案名为imc

[WX3010E-isp-dot1x]accounting lan-access radius-scheme imc

(3)#认证缺省域为dot1x

[WX3010E]domain default enable dot1x

#全局使能端口安全

[WX3010E]port-security enable

#设置802.1x的认证方式为EAP

[WX3010E]dot1x authentication-method eap

(4)#创建AP地址池

[WX3010E]dhcp server ip-pool ap

[WX3010E-dhcp-pool-ap]network 192.168.1.0 mask 255.255.255.0

[WX3010E-dhcp-pool-ap]gateway-list 192.168.1.1

#创建客户端地址池

[WX3010E]dhcp server ip-pool sta

[WX3010E-dhcp-pool-sta]network 192.168.10.0 mask 255.255.255.0

[WX3010E-dhcp-pool-sta]gateway-list 192.168.10.1

[WX3010E-dhcp-pool-sta]dns-list 9.9.9.9

(5)#配置无线接口WLAN-ESS1

#创建接口WLAN-ESS1并进入其视图

interface WLAN-ESS1

#接口WLAN-ESS1下放通对应的业务vlan

[WX3010E-WLAN-ESS1]port access vlan 10

#WLAN-ESS 1 上使能802.1x端口安全模式

[WX3010E-WLAN-ESS1]port-security port-mode userlogin-secure-ext

#在接口WLAN-ESS1下使能11key类型的密钥协商功能

[WX3010E-WLAN-ESS1]port-security tx-key-type 11key

#关闭dot1x握手模式

[WX3010E-WLAN-ESS1]undo dot1x handshake

#dot1x强制认证域为dot1x

[WX3010E-WLAN-ESS1]dot1x mandatory-domain dot1x

(6)#无线服务模板配置

#创建crypto类型的服务模板1并进入其视图

[WX3010E]wlan service-template 1 crypto

#设置当前服务模板的SSID（服务模板的标识）为h3c-1x

[WX3010E-wlan-st-1]ssid h3c-1x

#将WLAN-ESS1接口绑定到服务模板1

[WX3010E-wlan-st-1]bind WLAN-ESS 1

#使能TKIP加密套件

[WX3010E-wlan-st-1]cipher-suite tkip

#设置在AP发送信标和探查响应帧时携带WPA IE

[WX3010E-wlan-st-1]security-ie wpa

#使能服务模板

[WX3010E-wlan-st-1]service-template enable

(7)#创建相应的vlan三层虚接口

#创建管理vlan 三层接口

[WX3010E]interface Vlan-interface1

[WX3010E-Vlan-interface1]ip address 192.168.1.1 255.255.255.0

#创建业务vlan 三层接口

[WX3010E]interface Vlan-interface10

[WX3010E-Vlan-interface10]ip address 192.168.10.1 255.255.255.0

#创建连接服务器vlan 三层接口，即nas-ip地址

[WX3010E]interface Vlan-interface100

[WX3010E-Vlan-interface100]ip address 10.153.43.141 255.255.255.0

2、SW侧配置（略）

3、IMC 步骤配置

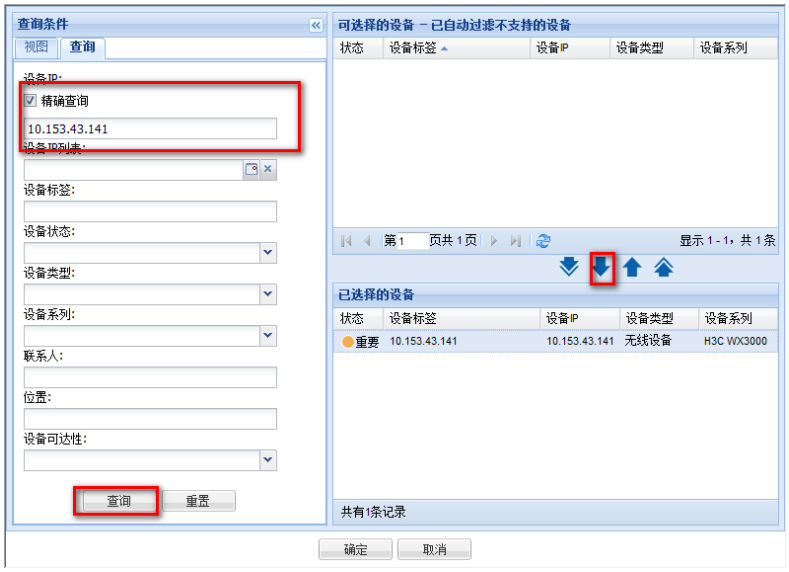
1. 接入设备配置：

#登录iMC平台，点击“资源”->“增加设备”。

#IP地址10.153.43.141，并配置SNMP和Telnet参数，和AC上snmp-agent和local-user(服务类型telnet)配置一致，点击“确定”。

#点击“用户”-> “接入策略管理” -> “接入设备管理”，选择“选择”。

输入设备地址10.153.43.141，精确查找，添加对应设备到“已选择的设备中”，点击“确定”。

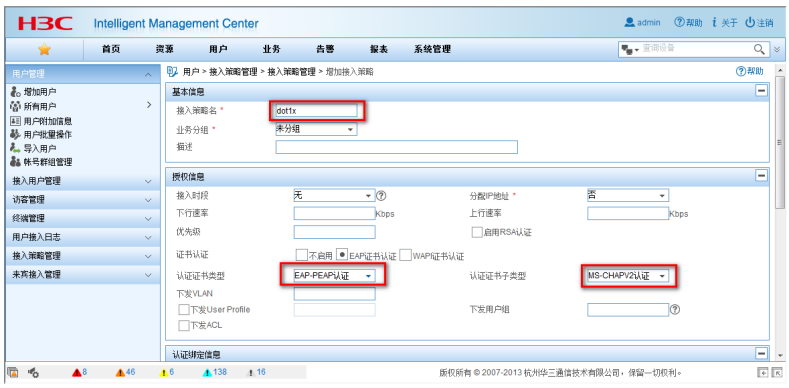


#选择“确定”。

2.创建dot1x策略

#选择“用户”-> “接入策略管理” -> “接入策略管理”，选择“增加”。

#输入策略名h3c-dot1x，选择“EAP证书认证”，证书类型“EAP-PEAP”，子类型“MS-CHAPV2”，点击“确定”。



选择“用户”-> “接入策略管理” -> “接入服务管理”，选择“增加”。填写服务名dot1x，接入策略选择“dot1x”，点击“确定”。

#选择“用户”-> “用户管理” -> “增加用户”。用户姓名dot1x，证件号码01010101，点击“确定”。

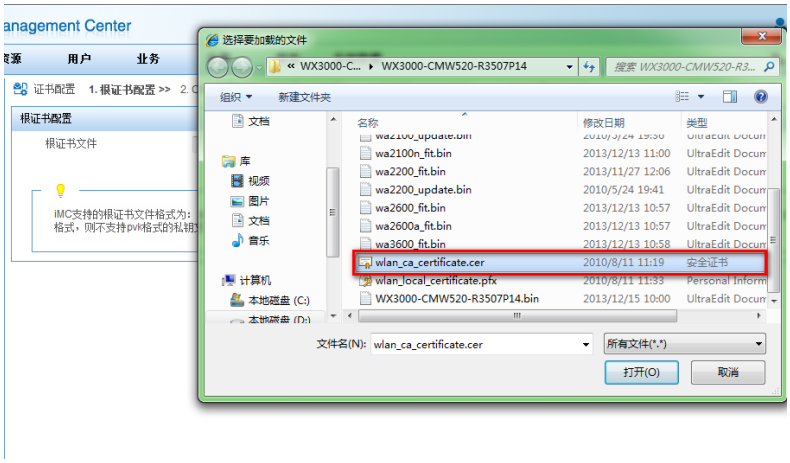
#选择“增加接入用户”，账户名dot1x，密码，勾选“dot1x”服务，点击“确定”。

3．证书导入配置：

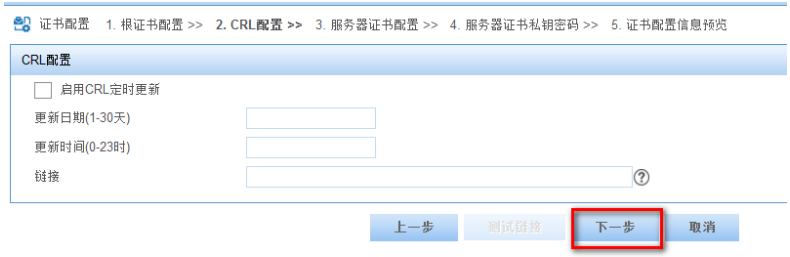
#选择“用户”-> “接入策略管理” -> “业务参数配置”->“证书配置”，选择“EAP证书配置”。

#选择对应的根证书和服务器证书，选择“下一步”，最后点击“确定”。注：根证书和服务器证书选择AC接入设备当前版本匹配的根证书和服务器证书。

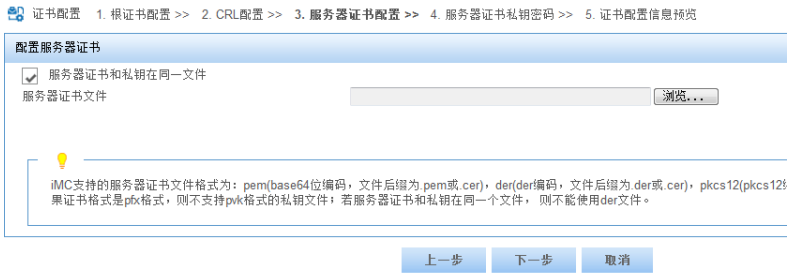
点击“浏览”，在PC上找到和AC版本对应的根证书，选择“打开”，如我的AC版本号为WX3000-CMW520-R3507P14，内部版本号为V300R005B09D020。

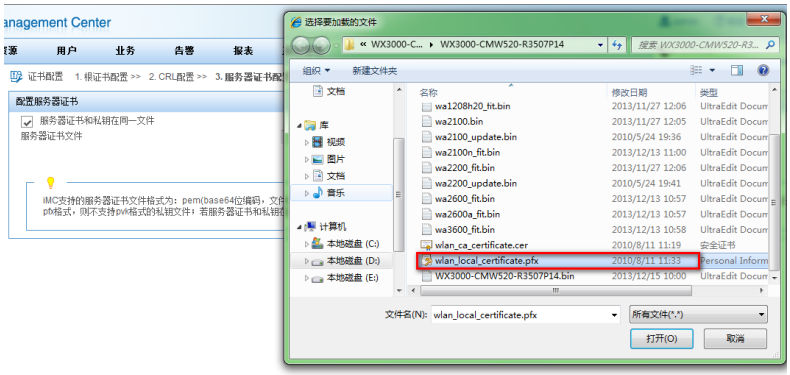


#选择“下一步”。

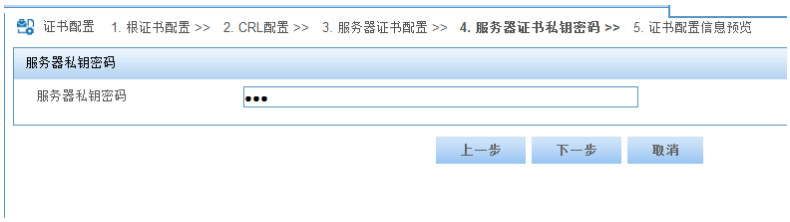


#点击“浏览”，选择服务器证书。





#输入服务器私钥密码：h3c，选择“下一步”。



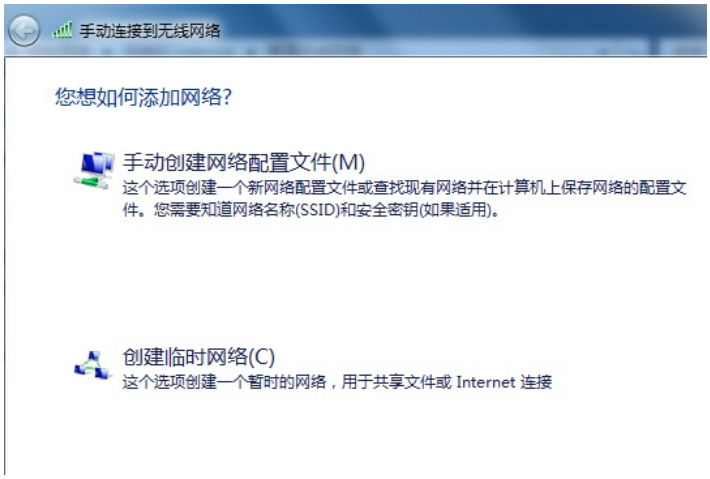
#选择“确认”。

三、客户端配置

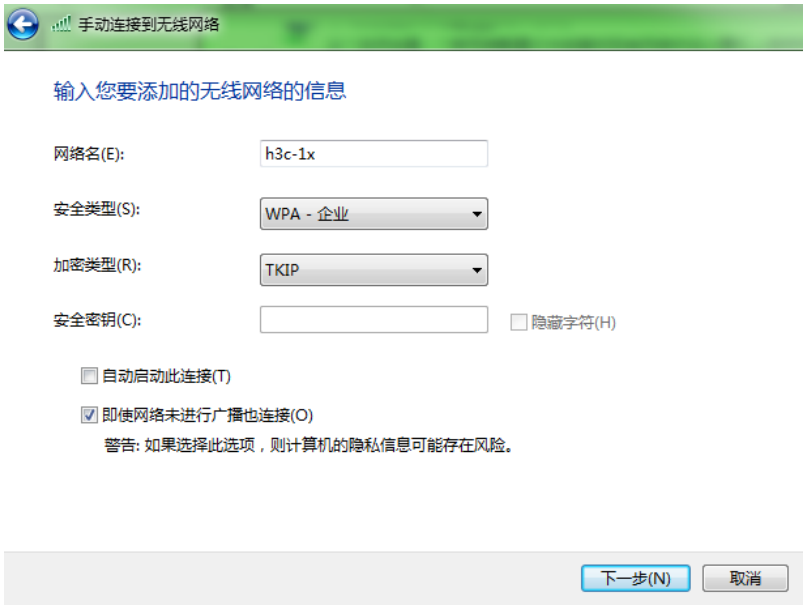
1.STA配置：

#进入网络和共享中心，选择“管理无线网络”。

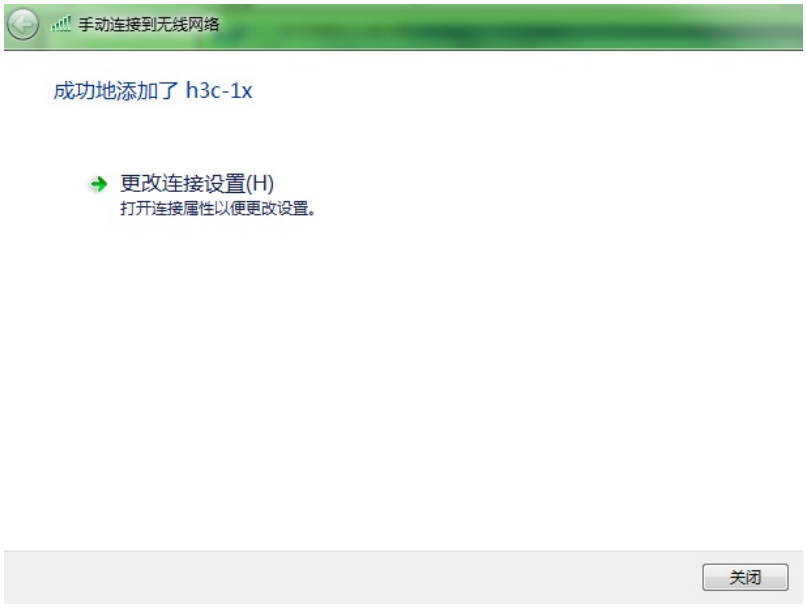
选择“添加”，# 选择“手动创建网络配置文件”。



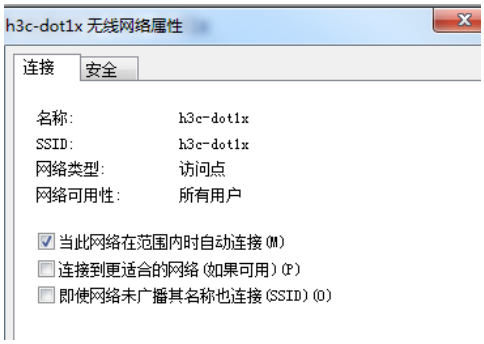
#输入SSID :h3c-1x，安全类型WPA，加密类型TKIP，选择“下一步”。



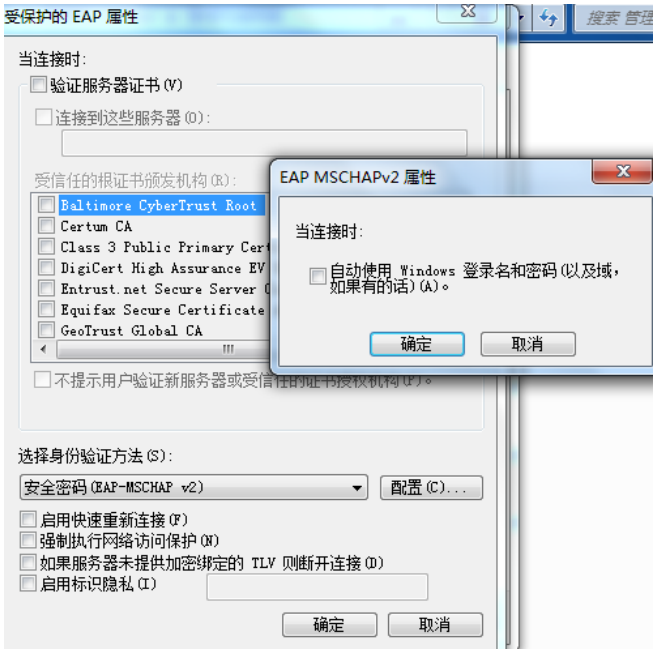
#选择“更改连接设置”。



#点击“安全”。



#选择“设置”，进入“配置”，去掉所有勾选，并点击“确定”。



#找到ssid=h3c-1x，点击连接即可。

四、实验结果验证

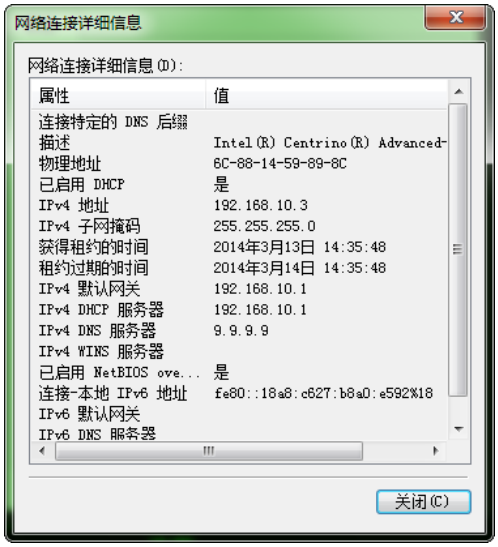
1、认证成功后，AC侧显示客户端信息

```
<WX3010E>dis connection

Index=36   ,Username=dot1x@dot1x
MAC=6C-88-14-59-89-8C
IP=192.168.10.3
IPv6=N/A
Online=00h02m34s
 Total 1 connection(s) matched.
<WX3010E>sy
System View: return to User View with Ctrl+Z.
[WX3010E]dis wlan c
[WX3010E]dis wlan client
 Total Number of Clients         : 1
                        Client Information
 SSID: h3c-1x
--------------------------------------------------------------------------------
MAC Address    User Name           APID/RID IP Address                   VLAN
--------------------------------------------------------------------------------
6c88-1459-898c dot1x               1   /2   192.168.10.3                 10
--------------------------------------------------------------------------------
```

```
<WX3010E>dis wlan client verbose
 Total Number of Clients          : 1
                          Client Information
--------------------------------------------------------------------------------
 MAC Address                      : 6c88-1459-898c
 User Name                        : dot1x
 IP Address                       : 192.168.10.3
 AID                              : 1
 AP Name                          : ap1
 Radio Id                         : 2
 Antenna Id                       : 0
 Service Template Number          : 1
 SSID                             : h3c-1x
 BSSID                            : 5866-ba5e-c6f0
 Port                             : WLAN-DBSS1:2
 VLAN                             : 10
 State                            : Running
 Power Save Mode                  : Active
 Wireless Mode                    : 11g
 QoS Mode                         : WMM
 Listen Interval (Beacon Interval) : 100
 RSSI                             : 67
 Rx/Tx Rate                       : 48/54
 Client Type                      : WPA
 Authentication Method            : Open System
 Authentication Mode              : Central
 AKM Method                       : Dot1X
 4-Way Handshake State            : PTKINITDONE
 Group Key State                  : REKEYESTABLISHED
 Encryption Cipher                : TKIP
 Roam Status                      : Normal
 Roam Count                       : 0
 Up Time (hh:mm:ss)               : 00:09:31
```

2、客户端信息



3、认证成功之后，客户端能ping 通网关