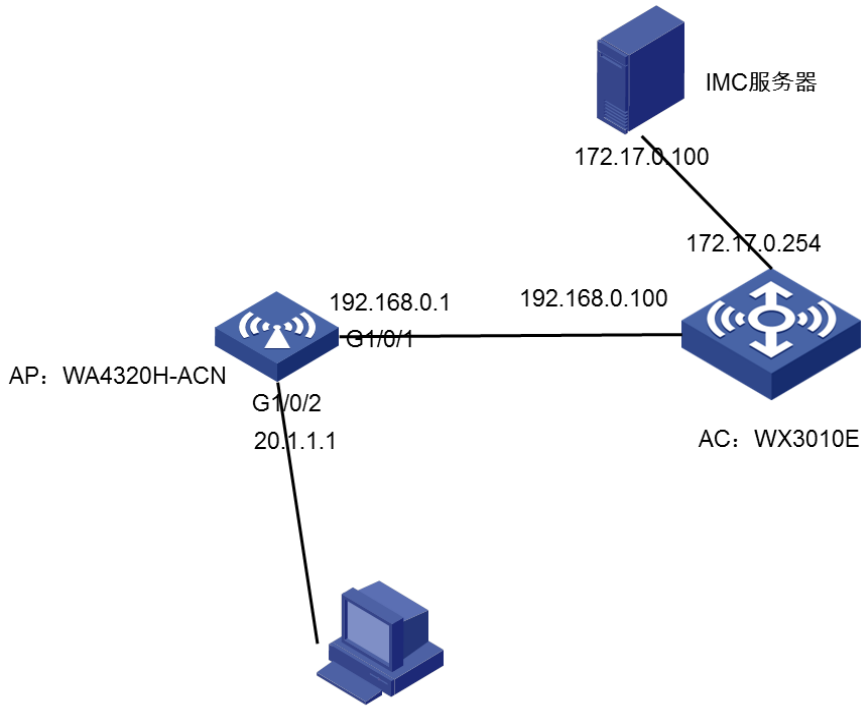
基于面板APWA4320H-ACN的有线802.1x认证典型配置

wlan接入 802.1X 杨攀 2015-10-22 发表

IEEE802 LAN/WAN委员会为解决无线局域网网络安全问题，提出了802.1x协议。后来，802.1x协议作为局域网端口的一个普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。

802.1x协议是一种基于端口的网络接入控制协议（Port Based Network Access Control）。“基于端口的网络接入控制”是指在局域网接入设备的端口这一级对所接入的用户设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。



本配置举例中，使用WX3010E作为无线控制器，版本号为WX3000-CMW520-R3509P44 ，内部版本号是COMWAREV500R002B109D039，WA4320H-AGN作为AP，imc服务器作为802.1x。AC作为AP网关（vlan-interface1:192.168.1.100/24）并配置DHCP server为AP分配IP地址为192.168.0.1。

一、AP侧配置

注：AP注册上之后通过Telnet到AP上进行配置。

配置各接口的IP地址（略）。

system-view

配置dot1x的认证为EAP

dot1x authentication-method eap

创建RADIUS方案radius1并进入其视图。

[Sysname] radius scheme dot1x

设置主认证/计费RADIUS服务器的IP地址。

[Sysname-radius-radius1] primary authentication 172.17.0.100

[Sysname-radius-radius1] primary accounting 172.17.0.100

设置系统与认证RADIUS服务器交互报文时的共享密钥。

[Sysname-radius-radius1] key authentication h3c

设置系统与计费RADIUS服务器交互报文时的共享密钥。

[Sysname-radius-radius1] key accounting h3c

指示系统从用户名中去除用户域名后再将之传给RADIUS服务器。

[Sysname-radius-radius1] user-name-format without-domain

[Sysname-radius-radius1] quit

创建域aabbcc.net并进入其视图。

[Sysname] domain dot1x

指定radius1为该域用户的RADIUS方案，并采用local作为备选方案。

[Sysname-isp-aabbcc.net] authentication default radius-scheme dot1x

[Sysname-isp-aabbcc.net] authorization default radius-scheme dot1x

[Sysname-isp-aabbcc.net] accounting default radius-scheme dot1x

配置域dot1x为缺省用户域。

[Sysname] domain default enable dot1x

开启全局802.1x特性。

[Sysname] dot1x

开启指定端口GigabitEthernet 2/0/1的802.1x特性。

[Sysname] interface GigabitEthernet 1/0/2

[Sysname- GigabitEthernet 1/0/2] dot1x

[Sysname- GigabitEthernet 1/0/2] quit

二、AC侧配置

第一步：检查AC的里面的默认版本支持不支持所连接的AP，如果对应则可以进行下一步，如果不对应则重新更换设备。（通常在官网上查看软件版本说明即可）

第二步：配置AC

1、配置AP与AC属于VLAN1，VLAN1网关IP地址和DHCP Server在AC上：

[AC] interface Vlan-interface1

[AC-Vlan-interface1] ip address 192.168.0.100 255.255.255.0

[AC] dhcp server ip-pool vlan1　这个地址池是给AP下发地址的。

[AC-dhcp-pool-vlan1] network 192.168.0.0 mask 255.255.255.0

[AC-dhcp-pool-vlan1] gateway 192.168.0.100

2、使用二层注册方式即可，保证AP可以正确获得IP地址，在AC上配置AP模板、接入服务模板，检验AC对AP的管理能力：

[AC] wlan service-template 1 clear　配置服务模板1，明文的。

[AC-wlan-st-1] ssid h3c-1　　SSID：h3c-1

[AC-wlan-st-1] bind WLAN-ESS 1　　绑定ESS信道1，这个是用户STA和AC之间用的

[AC-wlan-st-1] authentication-mothod open-system

[AC-wlan-st-1] service-template enable 开启服务模板

[AC] int WLAN-ESS 1

[AC-WLAN-ESS1] port access vlan 2

[AC] wlan ap ap model WA4320H-ACN　配置AP模板

[AC-wlan-ap-ap] serial-id 210235A29EB092002600

[AC-wlan-ap-ap] radio 1　radio代表射频卡

[AC-wlan-ap-ap-radio-1] service-template 1　关联服务模板

[AC-wlan-ap-ap-radio-1] radio enable　开启射频卡

第三步：

交换网板和业务网板上需要建立trunk链路，让所有的VLAN都能通过

AC上：interface Bridge-Aggregation 1

port link-type trunk

port trunk permit vlan all

第四步：

给STA配置DHCP服务器，且下发IP地址

[AC] vlan 2

[AC-vlan2] quit

[AC] interface Vlan-interface 2

[AC-Vlan-interface1] ip address 192.168.1.254 255.255.255.0

[AC] dhcp server ip-pool vlan2　　这个地址池是给STA下发的地址。

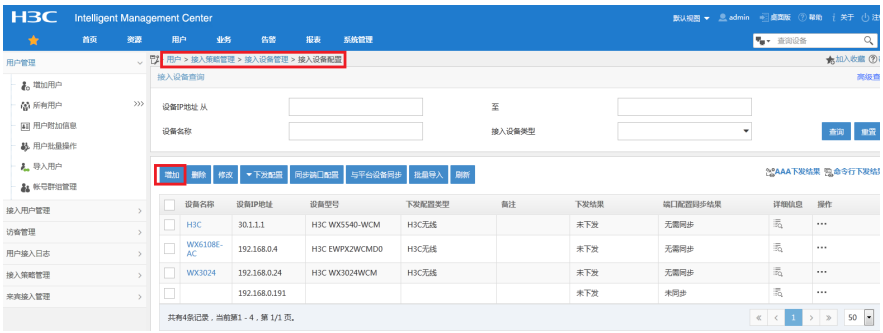
[AC-dhcp-pool-vlan1] network 192.168.1.0 mask 255.255.255.0

[AC-dhcp-pool-vlan1] gateway – list 192.168.1.254

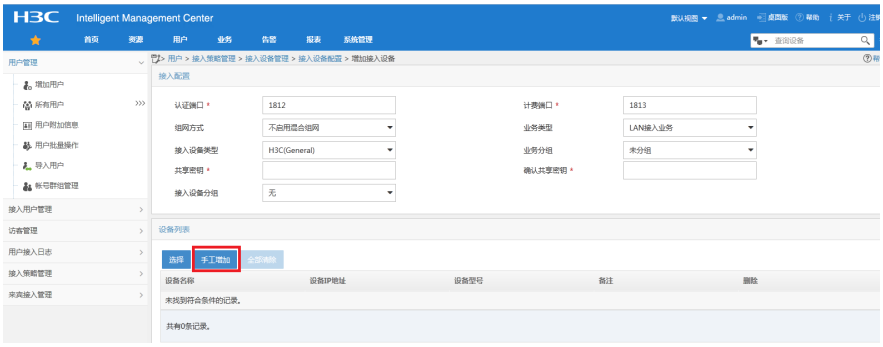
三、IMC配置

3.1、接入设备配置

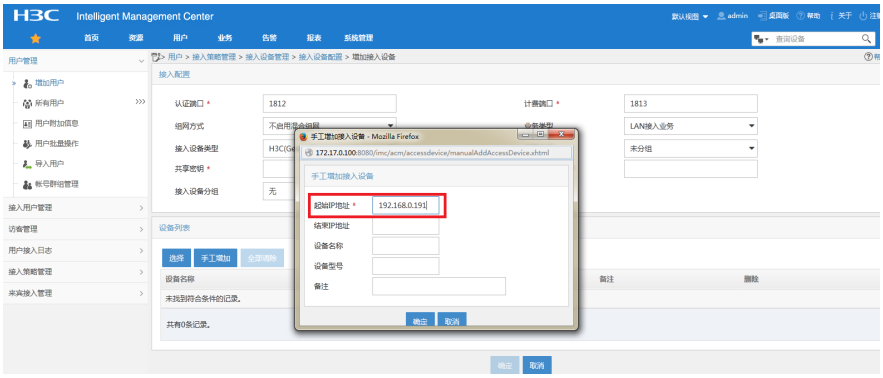
#登录IMC平台，点击“资源”->“接入策略管理”->“接入设备管理”->“接入设备配置”，选择增加



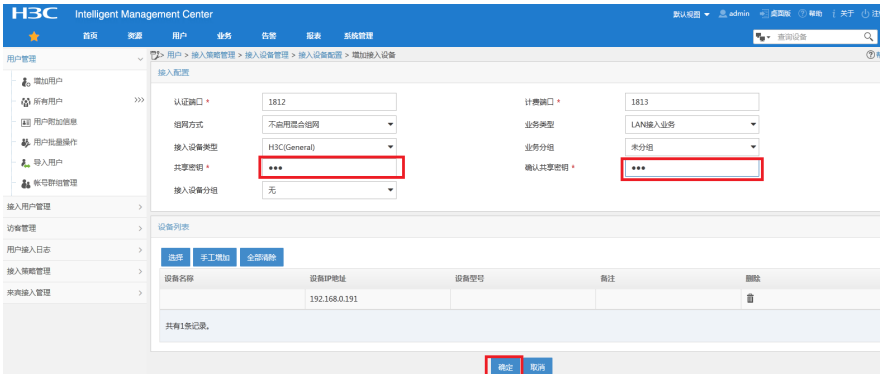
#点击“手工增加”



#输入设备地址192.168.0.191，点击“确定”

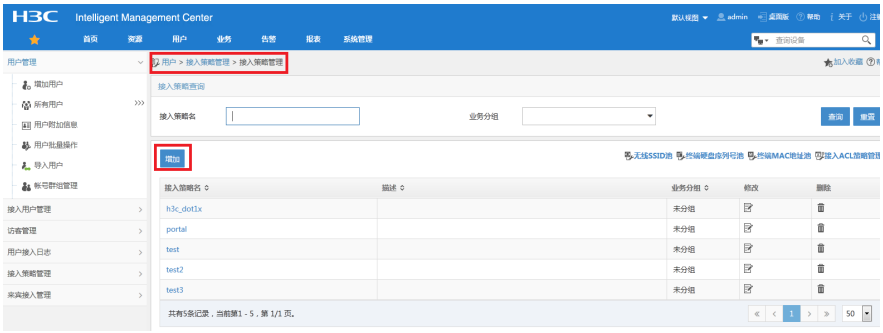


#配置共享秘钥“h3c”，点击“确定”

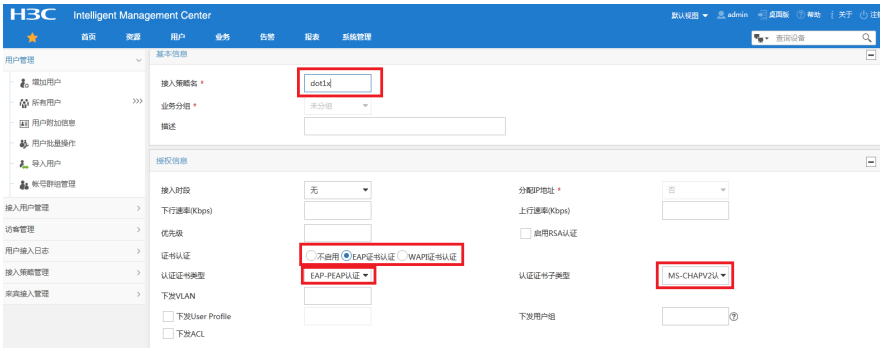


3.2、创建dot1x策略

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

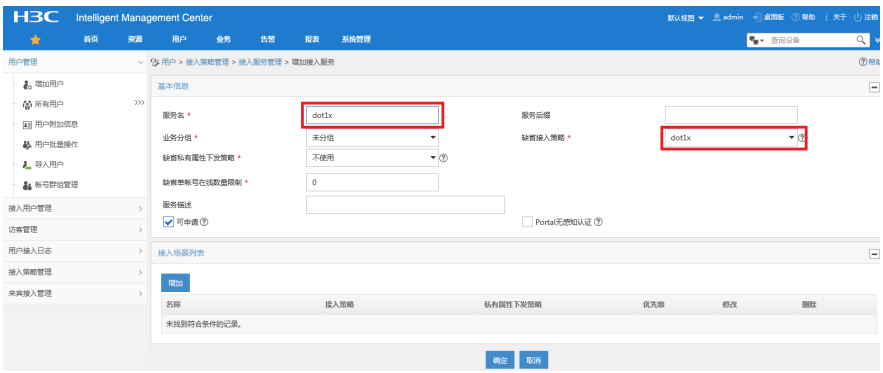


#输入策略名h3c-dot1x，选择“EAP证书认证”，证书类型“EAP-PEAP”，子类型“MS-CHAPV2”，点击“确定”。

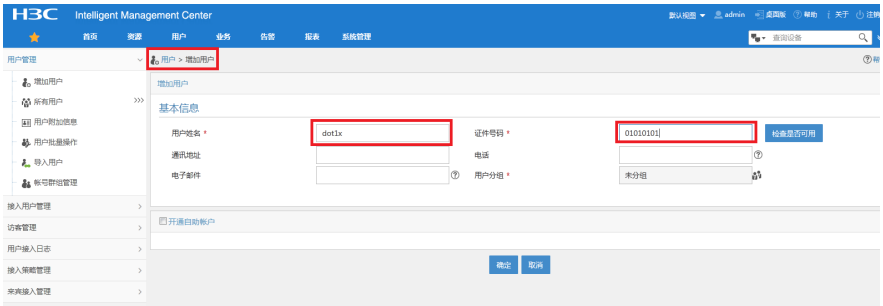


选择“用户”-> “接入策略管理” -> “接入服务管理”，选择“增加”。

#填写服务名dot1x，接入策略选择“dot1x”，点击“确定”。

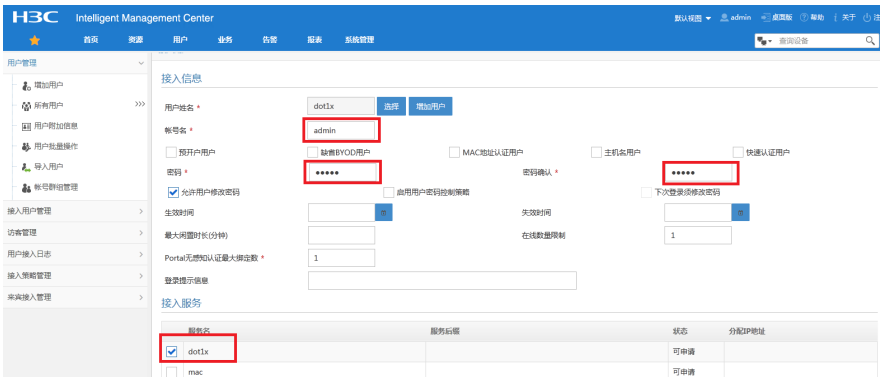


#选择“用户”-> “增加用户”。用户姓名dot1x，证件号码01010101，点击“确定”。



#选择“增加接入用户”

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

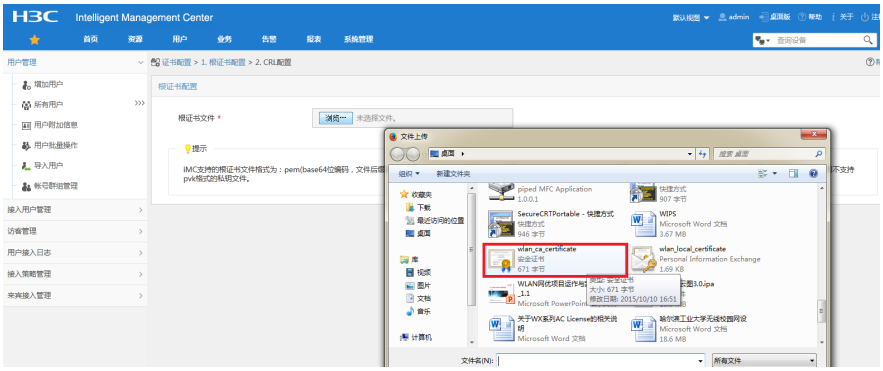


3.3、证书导入配置

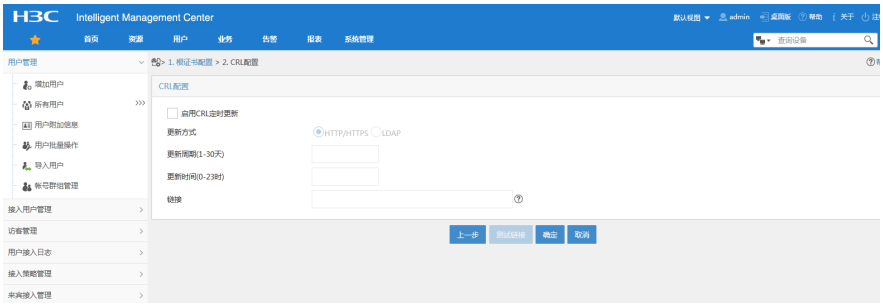
#选择“用户”-> “接入策略管理” -> “业务参数配置”->“证书配置”，选择“导入EAP根证书”

#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”，我的AC版本号为WX3000-CMW520-R3509P44 ，内部版本号是COMWAREV500R002B109D039



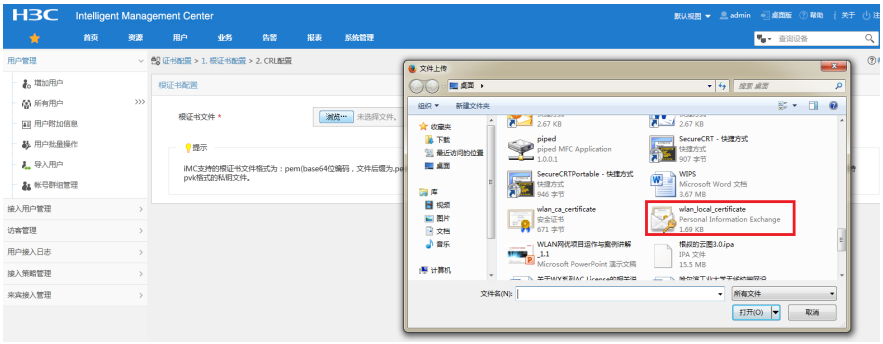
#点击“下一步”



#点击“确定”

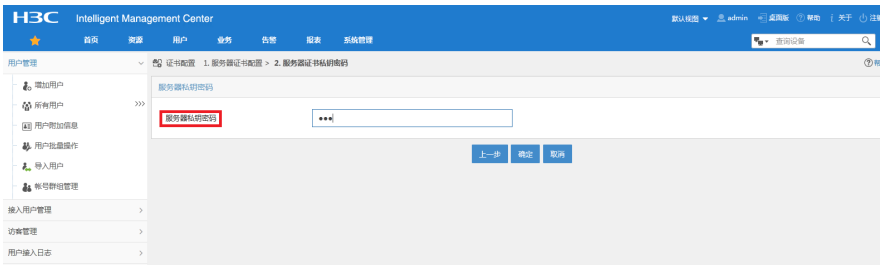
#点击“导入EAP根证书”

#点击“服务器和根证书在同一个文件”，点击“浏览”，导入服务器根证书。



#点击“打开”

#点击“下一步”

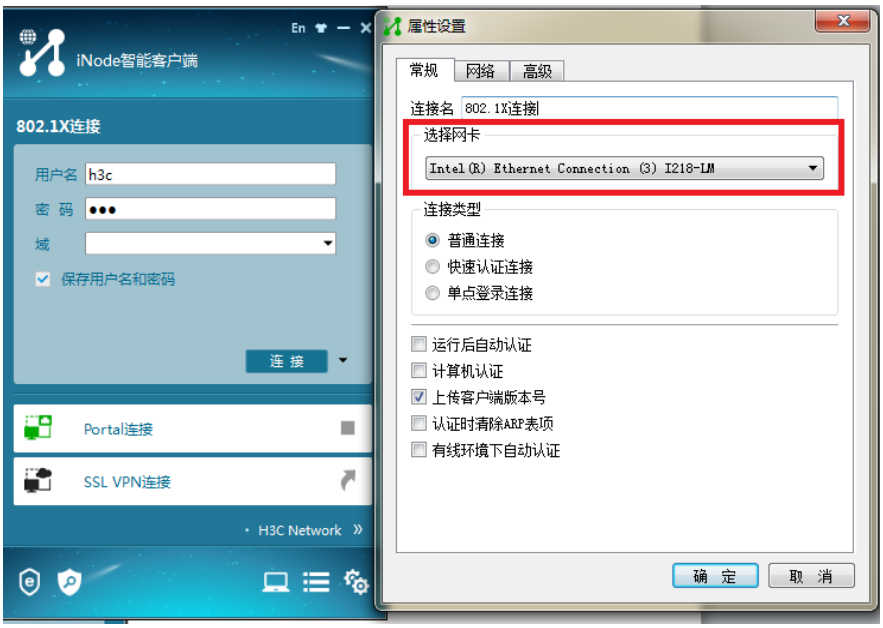


#输入服务器私钥“h3c”，点击“确定”

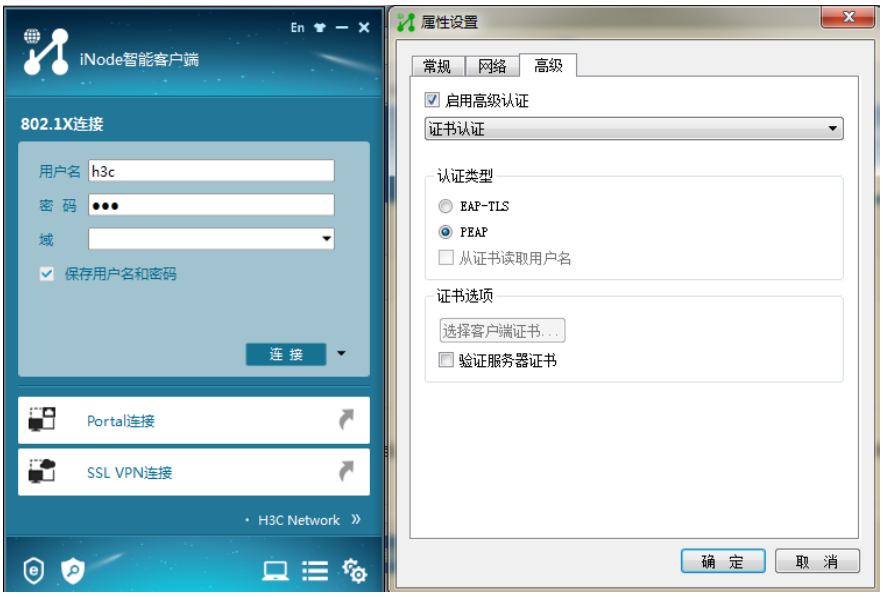
四、客户端配置

#双击iNode客户端，输入配置的用户名和密码，右击右下角的倒三角，点击“属性”

#选择网卡，更换为电脑的物理网卡，点击“确定”



#选择“高级”选项，“启用高级认证”，证书认证类型选择“PEAP”



#点击“确定”

五、验证

连接状态为“已连接”，表示连接成功。

六、配置注意事项

1、AP注册上之后通过Telnet或者console线登录上去进行配置

2、iMC和NAS设备路由可达；

3、iMC与NAS设备之间的UDP 1812,1813端口放通；

4、确保radius scheme *test*配置的共享密钥和iMC添加接入设备时配置的共享密钥一致

5、确保AC上配置portal server的共享秘钥和IMC上配置portal server的共享秘钥一致