

知 V7 WX系列产品远程802.1X认证配置案例（web版）

wlan安全 802.1X 樊凡 2020-03-08 发表

组网及说明

1 配置需求或说明

1.1 适用产品系列

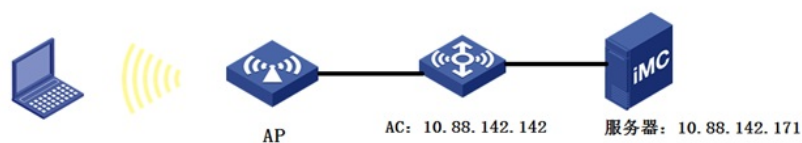
本案例适用于如WX1804H、WX2510H、WX3010H、WX3508H、WX5540H等WX18H、WX25H、WX30H、WX35H、WX55H系列的AC。

设备默认WAN口无地址，LAN口地址是192.168.0.100。

1.2 配置需求及实现的效果

无线电脑连接SSID：1x后，无线电脑自动获取192.168.39.0/24网段ip，网关vlan39的ip地址：192.168.39.1/24，想要实现对无线用户的统一管理和认证功能。现已有Radius服务器（10.88.142.171/24）提供认证服务，WX3510H使能远程802.1X认证，并作为无线网络的网关设备。客户端通过输入dot1x/123456这组账号密码进行认证登录，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，以iMC为AAA服务器，ip地址是：10.88.142.171。

2 组网图



配置步骤

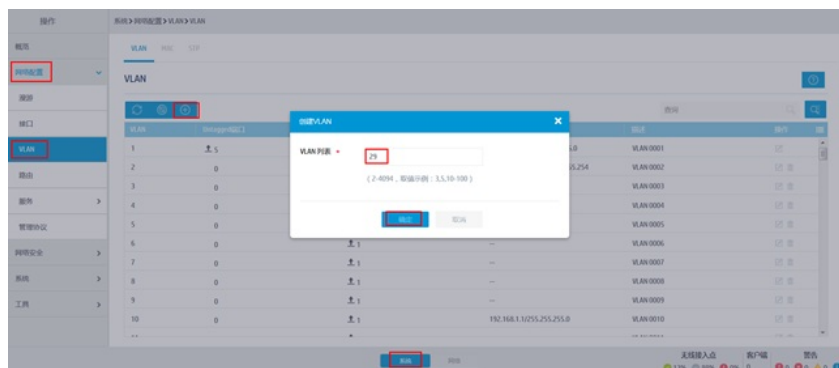
3 配置步骤

3.1 在无线控制器上配置相关VLAN及对应虚接口的地址

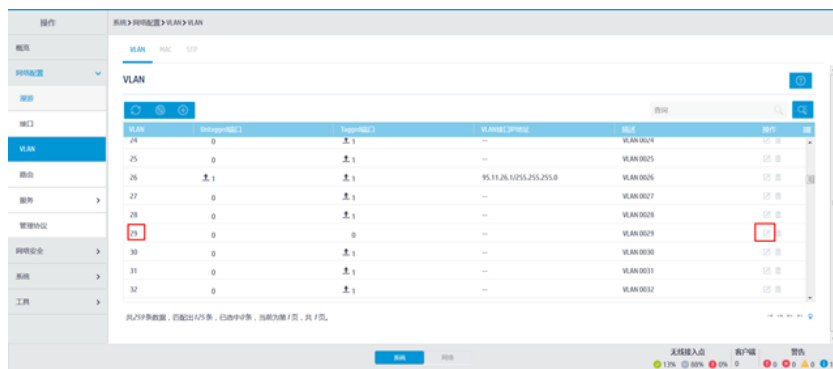
在AC上配置相关VLAN及对应虚接口的地址，并放通对应接口。

创建VLAN29及其对应的VLAN接口，并为该接口配置IP地址。开启dhcp服务，作为AP的管理vlan。

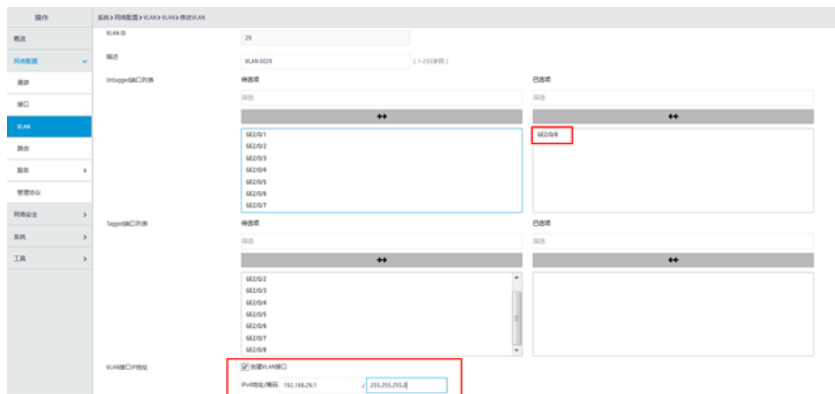
#在“系统”>“网络配置”>“VLAN”中创建vlan29。



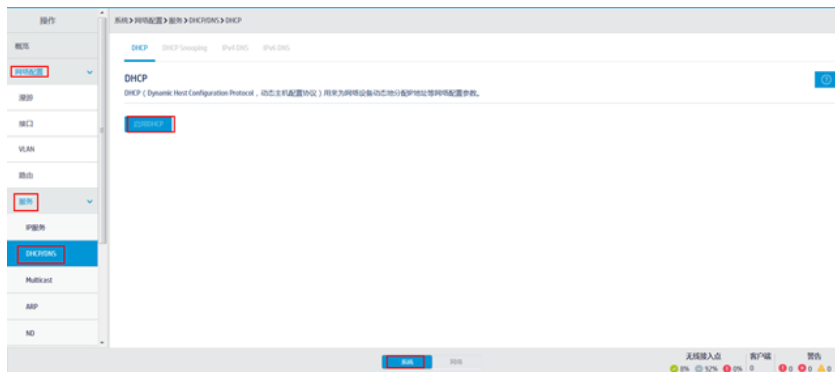
#创建vlan后，找到vlan29，点击“编辑”进去，进一步设置



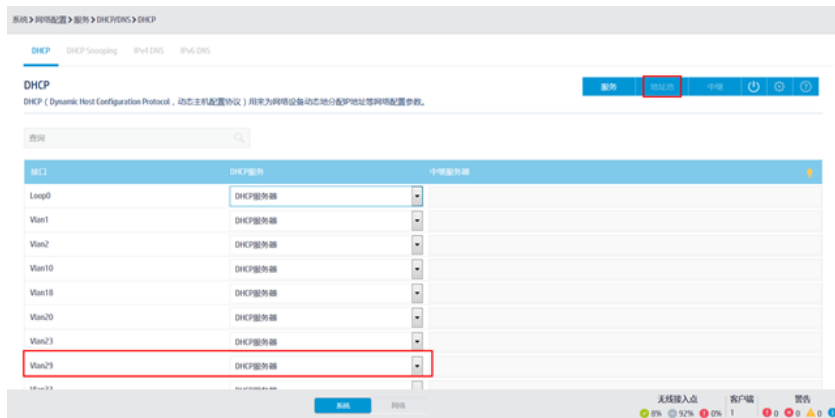
#由于G2/0/8接的是AP，vlan29为AP管理vlan，故此时需要将G2/0/8添加到untagged端口中。并且勾选创建vlan接口，给vlan虚接口配置ip地址为：192.168.29.1/24。



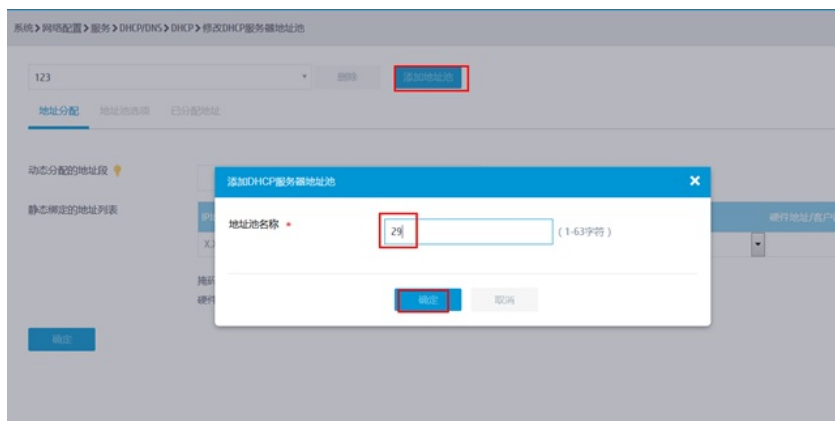
#在“系统”>“网络配置”>“服务”>“DHCP/DNS”>“DHCP”中开启DHCP服务器。



#点击“地址池”添加地址池。



#地址池名称设置为“29”。



#创建用于下发的网段地址，这个地址一定要和vlan29的IP地址在同一网段。

系统 > 网络配置 > 服务 > DHCP/DNS > DHCP > 修改DHCP服务器地址池

29 删除 添加地址池

地址分配 地址池选项 已分配地址

动态分配的地址段 192.168.29.0 / 255.255.255.0 (地址/掩码)

静态绑定的地址列表

IP地址	掩码	类型	硬件地址
X.X.X.X		以太网	

掩码长度范围必须为1到30。
硬件地址为4-39个字符的字符串。

确定

#在地址池中添加网关信息或者DNS信息，输入完成后一定要点击“+”符号添加。

系统 > 网络配置 > 服务 > DHCP/DNS > DHCP > 修改DHCP服务器地址池

29 删除 添加地址池

地址分配 地址池选项 已分配地址

租约有效期限 无限制

1 天 0 小时 0 分 0 秒

域名后缀 (1-50字符)

网关 192.168.29.1 X.X.X.X

DNS 服务器 114.114.114.114 X.X.X.X

WINS服务器 X.X.X.X

NetBIOS节点类型 请选择...

DHCP选项

创建VLAN39及其对应的VLAN接口，并为该接口配置IP地址。开启dhcp服务，Client使用该VLAN接入无线网络。具体操作同上，此处不再重复。

3.2 配置RADIUS方案

#点击“系统”>“网络安全”>“认证”>“RADIUS”，点击新增radius方案。

系统 > 网络安全 > 认证 > RADIUS

RADIUS

RADIUS方案用于定义设备和RADIUS服务器之间进行信息交互所必需的一些参数，例如：RADIUS服务器的IP地址、UDP端口号、报文共享密钥。

名称	认证服务器	计费服务器	操作
ss			编辑 删除
002	10.86.142.22:1812	10.86.142.22:1813	编辑 删除
01	10.86.142.22:1812		编辑 删除
portal	10.86.142.22:1812	10.86.142.22:1813	编辑 删除
shouhu	10.86.142.8:1812	10.86.142.8:1813	编辑 删除
test	10.153.68.75:1812	10.153.68.75:1813	编辑 删除
yportal	10.86.142.4:1812	10.86.142.4:1813	编辑 删除

共 10 条数据，已配置 10 条，已选中 0 条，当前为第 1 页，共 1 页。

新增 删除 重置 帮助

#配置RADIUS方案的主认证和主计费服务器及其通信密钥。

系统 > 网络安全 > 认证 > RADIUS

认证服务器

添加认证服务器

名称: [10.88.142.181] (1-32字符)

IP地址: 10.88.142.181 端口: 1812 认证协议: RADIUS 状态: 启用

计费服务器

添加计费服务器

名称: [10.88.142.181] (1-32字符)

IP地址: 10.88.142.181 端口: 1813 认证协议: RADIUS 状态: 启用

修改认证服务器

修改计费服务器

显示高级设置

#点击“显示高级设置”，配置发送给RADIUS服务器的用户名不携带ISP域名和radius报文发送的源地址。

修改后的计费共享密钥: [] (1-64字符)

发送RADIUS报文使用的源IPv4地址: 10.88.142.142

发送RADIUS报文使用的源IPv6地址: []

服务器响应超时时间: 3 秒 (1-10, 缺省为3)

发送RADIUS报文的最大尝试次数: 3 (1-20, 缺省为3)

服务器恢复活动状态的时间: 5 分钟 (1-255, 缺省为5)

发送实时计费更新报文的间隔: 720 秒 (0-71582, 缺省为720)

发起实时计费更新请求的最大尝试次数: 5 (1-255, 缺省为5)

发送给RADIUS服务器的用户名格式: 不携带域名

发送给RADIUS服务器的数据流的单位: 字节

发送给RADIUS服务器的数据包的单位: 包

Accounting-on: ☐ 开启Accounting-on功能

隐藏高级设置...

确定 取消

#点击“系统”>“网络安全”>“认证”>“RADIUS”，右上角“高级设置”。

操作

配置

网络配置

网络配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

配置

#使能RADIUS session control功能。

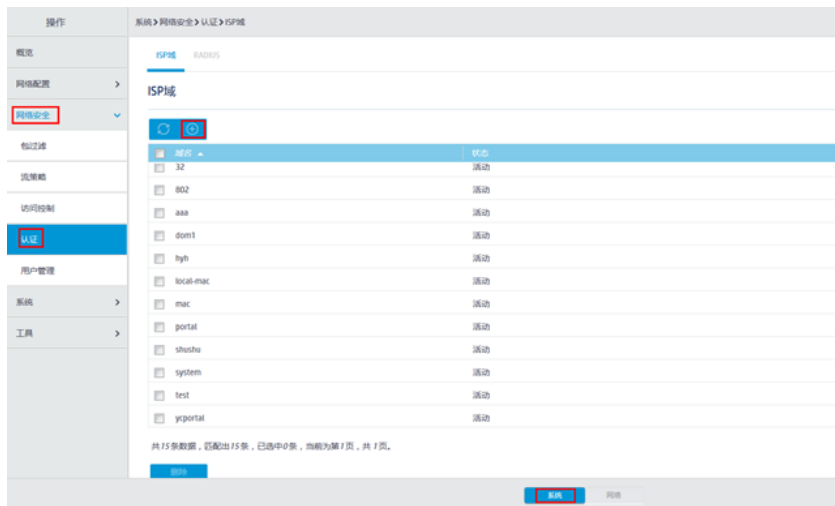
系统 > 网络安全 > 认证 > RADIUS

接收session control报文

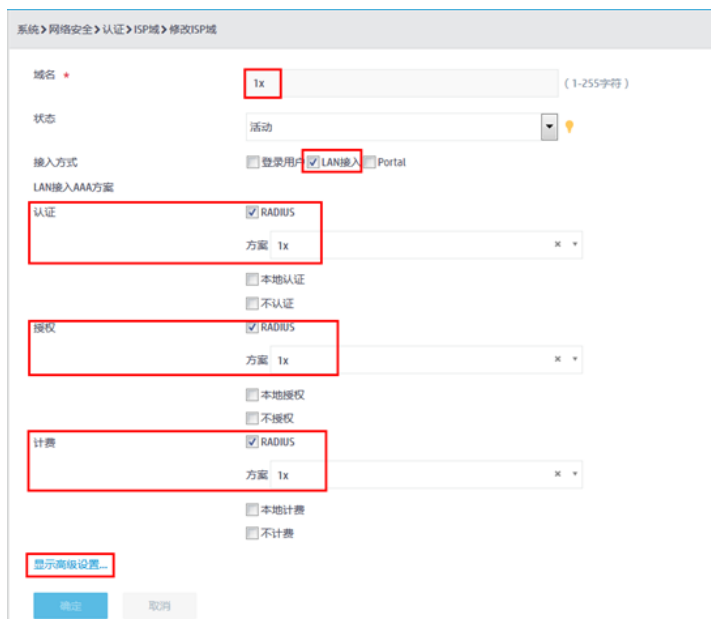
开

3.3 配置认证域

#点击“系统”>“网络安全”>“认证”>“ISP域”，新增ISP域。



#为dot1x用户配置AAA认证、授权和计费的方法为radius方案1x。

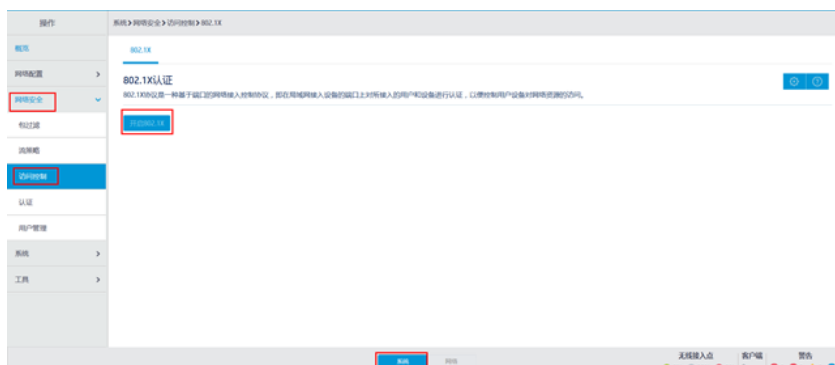


#指定1x域下的用户闲置切断时间为15分钟，闲置切断时间内产生的流量为1024字节。

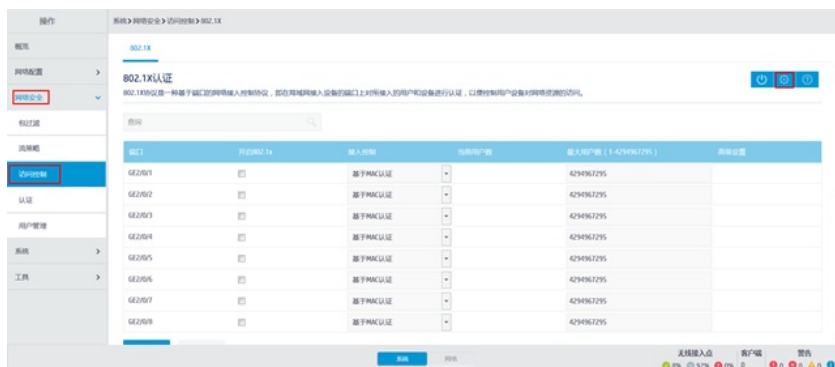


3.4 配置802.1X认证

#点击“系统”>“网络安全”>“访问控制”>“802.1X认证”，点击“开启802.1X”。



#点击右上角“高级设置”。



#配置802.1X系统的认证方法为EAP。

系统 > 网络安全 > 访问控制 > 802.1X

802.1X

认证方法 EAP

EAP

确定 取消

域名分隔符 @

周期性重认证时间间隔 3600秒

周期发送握手请求报文时间间隔 15秒

重发服务器认证请求报文时间间隔 100秒

重发客户端EAP-Request/MD5 Challenge请求报文时间间隔 30秒

重发客户端EAP-Request/Identity请求报文时间间隔 30秒

3.5 配置AP二层注册和无线服务

#点击“网络”>“无线配置”>“AP管理”>“AP”，点击新增。

AP ID	AP名称	AP型号	序列号	MAC地址	IP地址	状态	操作
12345678	AP01	WA5320-SI	219801A1B38197E00NWP	00-00-00-00-00-00	2.802.11a:00:00:00:00:00	在线	编辑 删除
12345679	AP02	WA5320-SI	219801A1B38197E00NWP	00-00-00-00-00-00	2.802.11a:00:00:00:00:00	在线	编辑 删除
12345680	AP03	WA5320-SI	219801A1B38197E00NWP	00-00-00-00-00-00	2.802.11a:00:00:00:00:00	在线	编辑 删除
12345681	AP04	WA5320-SI	219801A1B38197E00NWP	00-00-00-00-00-00	2.802.11a:00:00:00:00:00	在线	编辑 删除
12345682	AP05	WA5320-SI	219801A1B38197E00NWP	00-00-00-00-00-00	2.802.11a:00:00:00:00:00	在线	编辑 删除
12345683	AP06	WA5320-SI	219801A1B38197E00NWP	00-00-00-00-00-00	2.802.11a:00:00:00:00:00	在线	编辑 删除
12345684	AP07	WA5320-SI	219801A1B38197E00NWP	00-00-00-00-00-00	2.802.11a:00:00:00:00:00	在线	编辑 删除
12345685	AP08	WA5320-SI	219801A1B38197E00NWP	00-00-00-00-00-00	2.802.11a:00:00:00:00:00	在线	编辑 删除
12345686	AP09	WA5320-SI	219801A1B38197E00NWP	00-00-00-00-00-00	2.802.11a:00:00:00:00:00	在线	编辑 删除
12345687	AP10	WA5320-SI	219801A1B38197E00NWP	00-00-00-00-00-00	2.802.11a:00:00:00:00:00	在线	编辑 删除

#配置AP名称为ap10，型号名称选择WA5320-SI，并配置序列号219801A1B38197E00NWP。提示：此处根据实际的AP序列号来填写

AP名称 ap10

AP型号 WA5320-SI

序列号 219801A1B38197E00NWP

AP MAC地址 00-00-00-00-00-00

AP所在组名 default-group

认证模式 802.1X

AP连接方式 有线

CAPWAP隧道源 IP地址 192.168.1.1

隧道建立事件 事件名称 事件次数

Radius认证计费上报间隔 0-255

AP服务模板 开启 关闭

SSID策略 开启 关闭

Z-Radius认证 开启 关闭

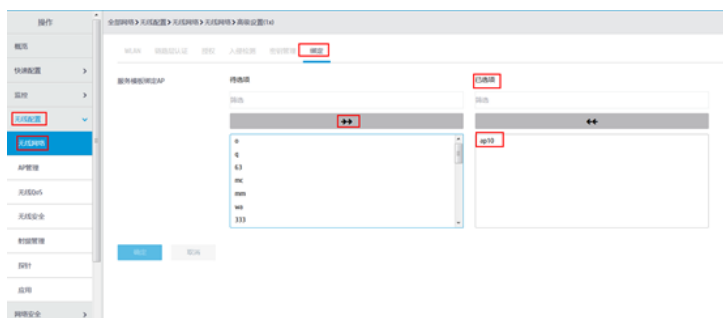
#选择“网络”>“无线配置”>“无线网络”中新增无线服务。设置无线SSID名称为“1x”，缺省vlan为vlan 39。并开启服务模板。认证模式选择为802.1X认证，认证域名为“1X”。



#点击“确认并进入高级设置”>“链路层认证”，按照如下截图操作。



#点击“绑定”，将“ap10”和无线服务模板“1x”做绑定，设置完成后点击确定。



3.6 配置客户端和服务器的连通性

#由于客户端网关就在AC上，且AC和服务器同网段。所以添加服务器侧 客户端192.168.39.0/24网段的路由即可，此处略。

3.7 Radius服务器设置

#下面以iMC为例（使用iMC版本为：iMC PLAT 7.1(E0303P16)），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（如图1）。在该页面中点击<增加>按钮（如图2），进入增加接入设备页面（如图3）。

·设置认证、计费共享密钥为123456，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10.88.142.142的接入设备。

图1接入设备页面

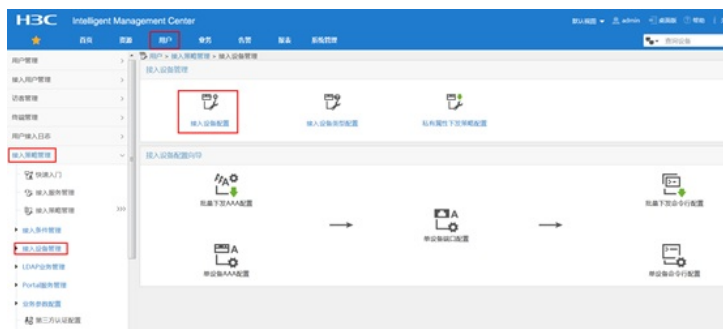
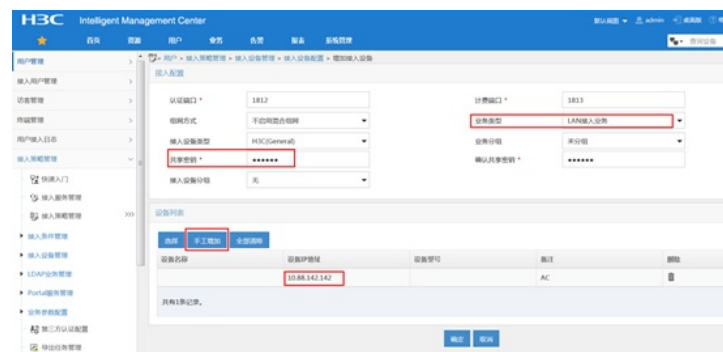


图2 点击增加



图3 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（如图4），进入增加接入策略页面（如图5）。

·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。

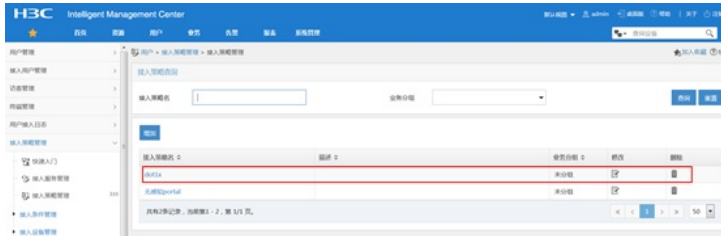
图4 选择增加接入策略



图5 增加接入策略页面



图6 成功添加接入策略dot1x



#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（如图7），进入增加接入服务页面（如图8）。

·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7 选择增加接入服务策略



图8 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（如图9），进入增加接入用户页面。

添加用户dot1x（如图10）；

添加账号名为dot1x，密码为123456（如图11）；

·选中之前配置的服务dot1x。

图9 选择增加接入用户

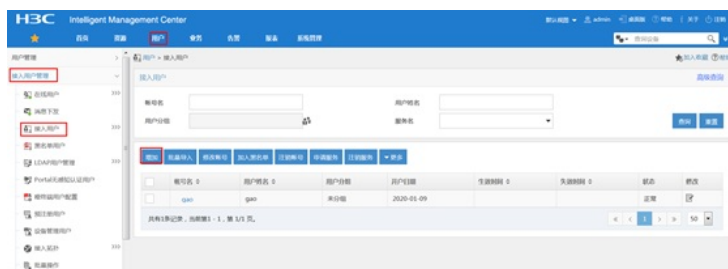


图10 添加用户dot1x

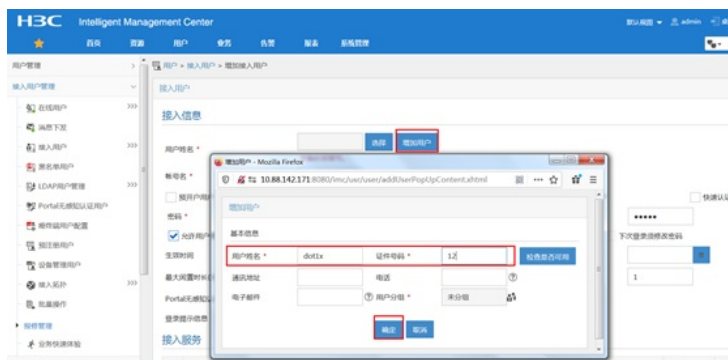


图11 增加接入用户界面

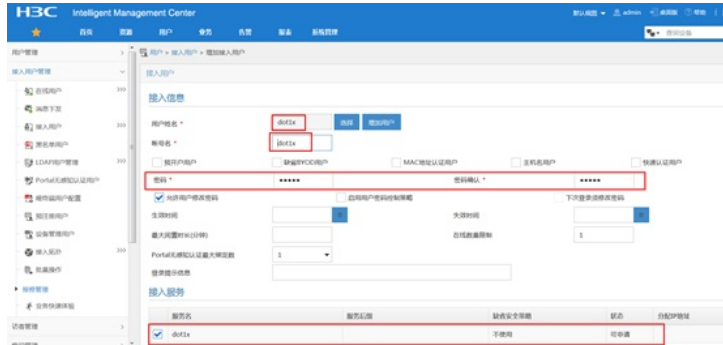
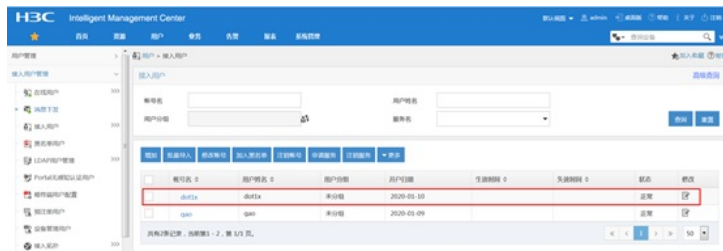


图12 创建接入用户dot1x成功



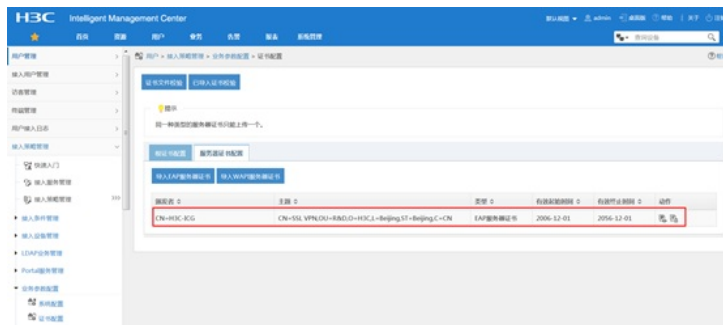
```
# 服务器侧导入证书。
```

选择“用户”页签，单击导航树中的[接入策略管理/业务参数配置/证书配置]菜单项，进入证书配置页面，在该页面中导入EAP根证书（如图13）和导入EAP服务器证书（如图14）。证书略。

图13 导入EAP根证书



图14 导入EAP服务器证书

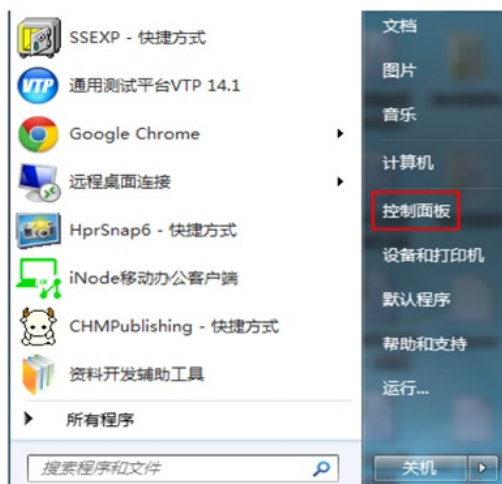


1.2 配置客户端

配置无线网卡

下面以Windows 7为例，说明无线网卡的配置。

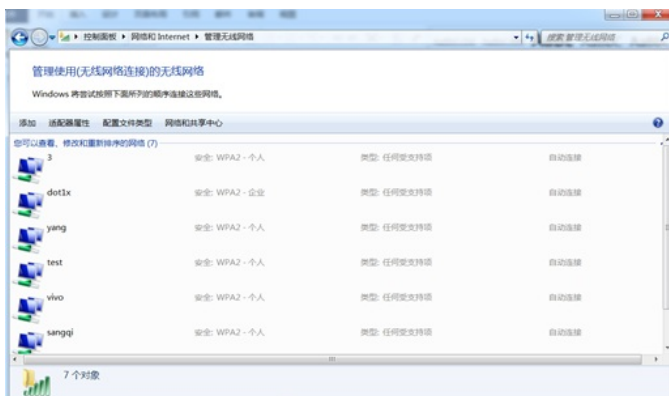
打开“开始”菜单，单击“控制面板”，进入控制面板窗口。



单击“查看网络状态和任务”，进入到了“网络和共享中心”。



单击“管理无线网络”，进入管理无线网络窗口。



单击<添加>按钮，选择“手动创建网络配置文件(M)”。



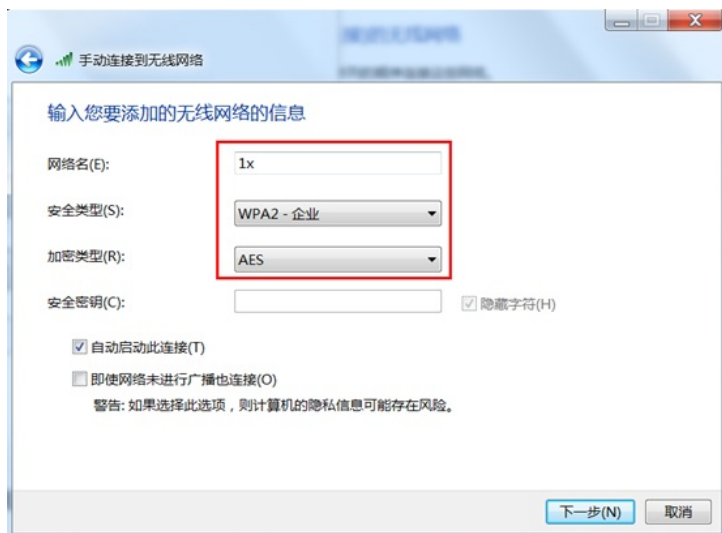
添加无线网络信息。

输入网络名(服务模板中的ssid): 1x;

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”。



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。

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。

单击<设置>按钮, 进入“保护的EAP属性”对话框。

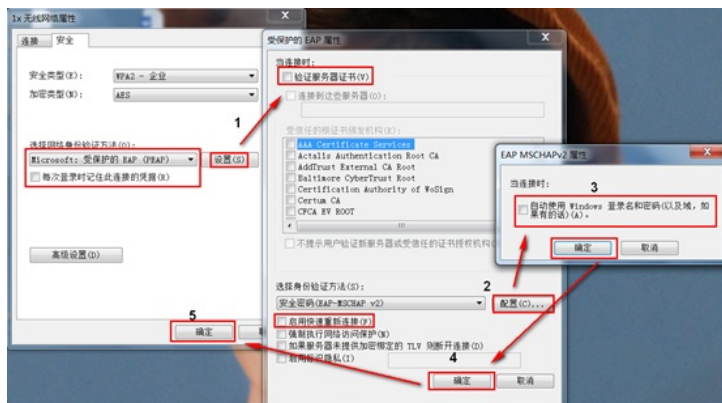
· 去掉“验证服务器证书(V)”前复选框中的勾;

· 去掉“启用快速重新连接”前复选框中的勾;

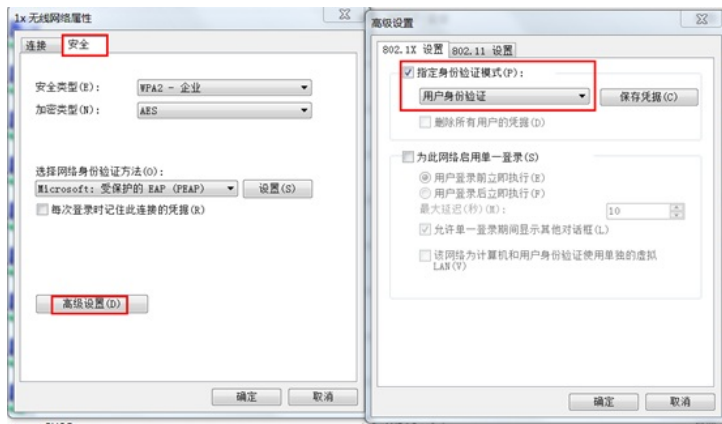
· 单击“选择身份验证方法(S)”后面的<配置>按钮;

· 在弹出的“EAP MSCHAPv2属性”对话框中, 去掉复选框中的勾;

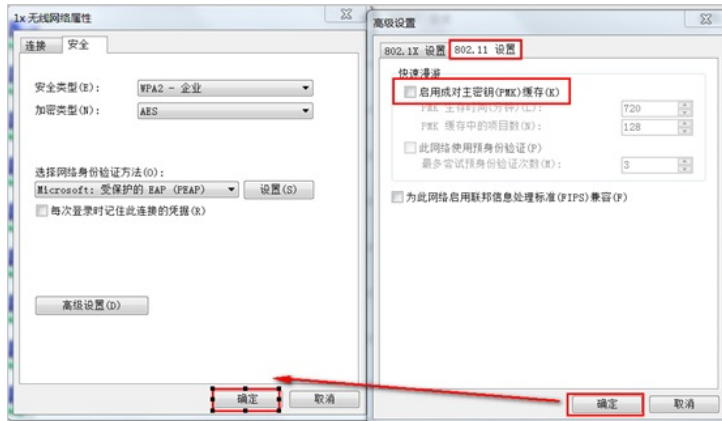
· 然后单击<确定>按钮, 返回“受保护的EAP属性”界面, 再单击<确定>按钮。



#选择“更改连接设置(H)”, 进入无线网络属性对话框。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”。

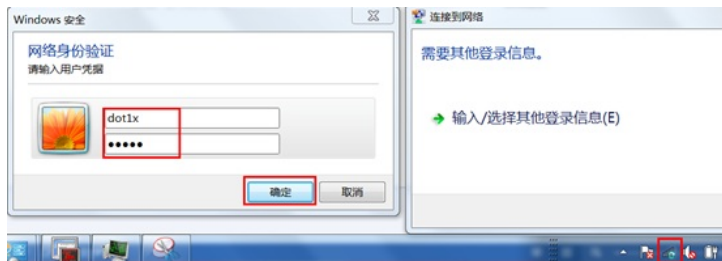


单击“802.11设置”页签，去掉“启用成对主密钥(PMK)缓存”前的复选框中的勾，然后单击<确定>按钮

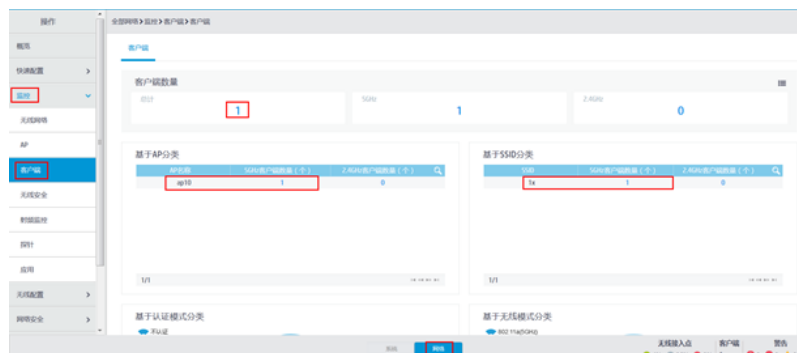


3.9 实验结果验证

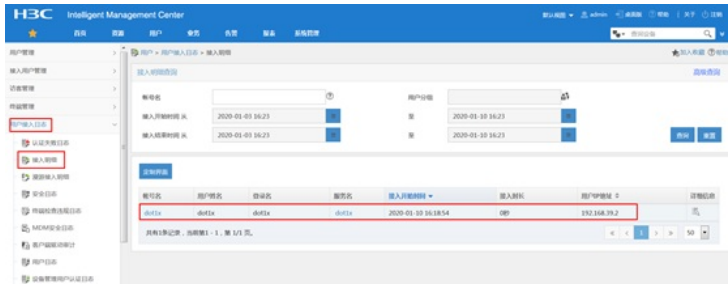
用电脑连接1x无线后，弹出一个登陆认证页面，需要输入认证账号：dot1x/123456通过认证后才能成功连接无线。



终端连上无线后获取到192.168.39.2的地址，在AC上查看客户端上线成功



在服务器侧同时能看到用户上线信息



配置关键点

无