WX系列产品远程802.1X认证配置案例（命令行版）

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

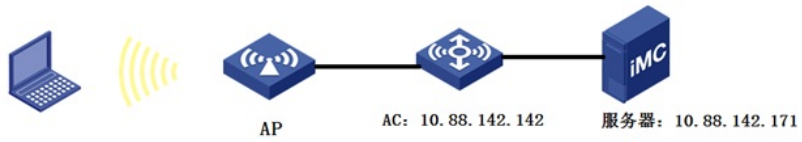
本案例适用于如WX1804H、WX2510H、WX3010H、WX3508H、WX5540H等WX18H、WX25H、WX30H、WX35H、WX55H系列的AC。

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。

system-view

[H3C] vlan 29

[H3C-vlan29] quit

[H3C] interface Vlan-interface 29

[H3C-Vlan-interface29] ip address 192.168.29.1 24

[H3C-Vlan-interface29] quit

#开启DHCP服务器功能

[H3C]dhcp enable

#配置地址池vlan29，分配192.168.29.0/24网段

[H3C]dhcp server ip-pool 29

[H3C-dhcp-pool-29]network 192.168.29.0 mask 255.255.255.0

#分配网关和DNS服务器地址，网关是192.168.29.1，DNS服务器是114.114.114.114。

[H3C-dhcp-pool-29]gateway-list 192.168.29.1

[H3C-dhcp-pool-29]dns-list 114.114.114.114

[H3C-dhcp-pool-29]quit

#配置AC与AP互连接口划分为vlan29。

[H3C] interface GigabitEthernet 1/0/10

[H3C- GigabitEthernet 1/0/10]port access vlan 29

[H3C- GigabitEthernet 1/0/10]quit

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

system-view

[H3C] vlan 39

[H3C-vlan39] quit

[H3C] interface Vlan-interface 39

[H3C-Vlan-interface39] ip address 192.168.39.1 24

[H3C-Vlan-interface39] quit

#开启DHCP服务器功能

[H3C]dhcp enable

#配置地址池vlan39，分配192.168.39.0/24网段

[H3C]dhcp server ip-pool 39

[H3C-dhcp-pool-39]network 192.168.39.0 mask 255.255.255.0
#分配网关和DNS服务器地址，网关是192.168.39.1，DNS服务器是114.114.114.114。
[H3C-dhcp-pool-39]gateway-list 192.168.39.1
[H3C-dhcp-pool-39]dns-list 114.114.114.114
[H3C-dhcp-pool-39]quit

3.2 配置RADIUS方案

配置radius认证,配置radius服务器的IP地址、秘钥及radius报文发送的源地址。
[H3C] radius scheme 1x
#配置RADIUS方案的主认证和主计费服务器及其通信密钥。
[H3C-radius-1x] primary authentication 10.88.142.171 key simple 123456
[H3C-radius-1x] primary accounting 10.88.142.171 key simple 123456
#配置发送给RADIUS服务器的用户名不携带ISP域名。
[H3C-radius-rs1] user-name-format without-domain
[H3C-radius-rs1] nas-ip 10.88.142.142
[H3C-radius-rs1] quit
#使能RADUIS session control功能。
[H3C] radius session-control enable

3.3 配置认证域

#创建名为1x的ISP域并进入其视图。
[H3C] domain 1x
#为dot1x用户配置AAA认证方法为RADIUS。
[H3C-isp-1x] authentication lan-access radius-scheme 1x
#为dot1x用户配置AAA授权方法为RADIUS。
[H3C-isp-1x] authorization lan-access radius-scheme 1x
#为dot1x用户配置AAA计费方法为RADIUS。
[H3C-isp-1x] accounting lan-access radius-scheme 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。
[H3C-isp-1x] authorization-attribute idle-cut 15 1024
[H3C-isp-1x] quit

3.4 配置802.1X认证

#配置802.1X系统的认证方法为EAP。
[H3C] dot1x
[H3C] dot1x authentication-method eap

3.5 配置AP二层注册和无线服务

#创建无线服务模板1x，并进入无线服务模板视图。
[H3C] wlan service-template 1x
#配置SSID为1x。
[H3C-wlan-st-1x] ssid 1x
#配置无线服务模板VLAN为39。
[H3C-wlan-st-1x] vlan 39
#配置身份认证与密钥管理的模式为802.1X。
[H3C-wlan-st-1x] akm mode dot1x
#配置CCMP为加密套件，配RSN为安全信息元素。
[H3C-wlan-st-1x] cipher-suite ccmp
[H3C-wlan-st-1x] security-ie rsn
#配置用户接入认证模式为802.1X。
[H3C-wlan-st-1x] client-security authentication-mode dot1x
配置802.1X用户使用认证域为1x。
[H3C-wlan-st-1x] dot1x domain 1x
#使能无线服务模板。
[H3C-wlan-st-1x] service-template enable
[H3C-wlan-st-1x] quit
#创建AP，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
[H3C] wlan ap ap10 model WA5320-SI
[H3C-wlan-ap-ap10] serial-id 219801A1B38197E00NWP
#进入Radio 1视图。
[H3C-wlan-ap-ap10] radio 1
#将无线服务模板1x绑定到radio 1，并开启射频。
[H3C-wlan-ap-office-radio-1] service-template 1x
[H3C-wlan-ap-office-radio-1] radio enable
[H3C-wlan-ap-ap10-radio-1] quit
[H3C-wlan-ap-ap10] quit

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

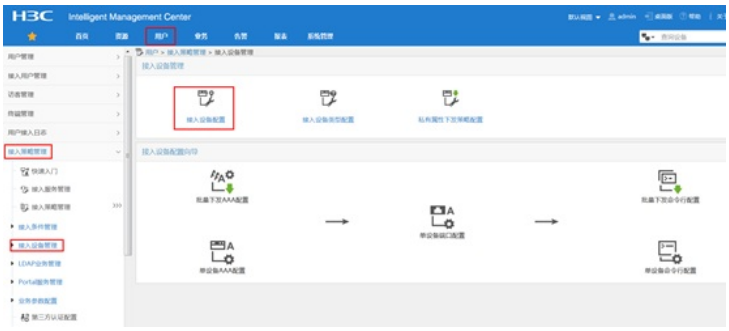
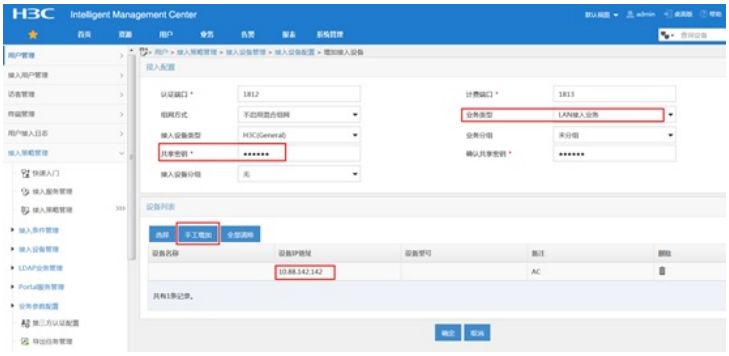


图2 点击增加

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

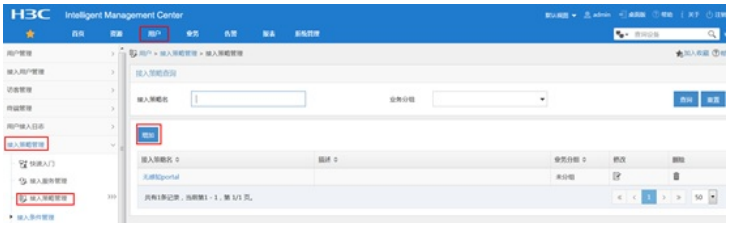


图5 增加接入策略页面

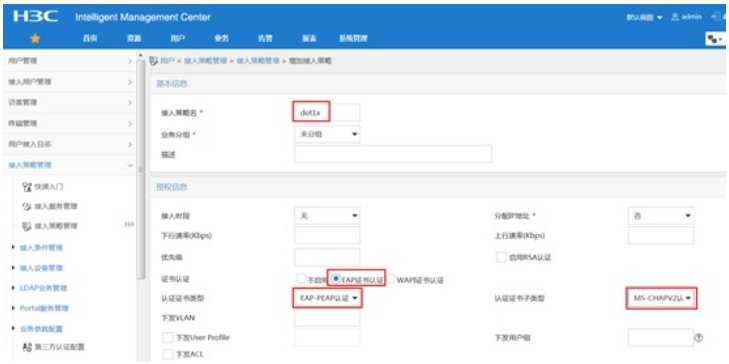
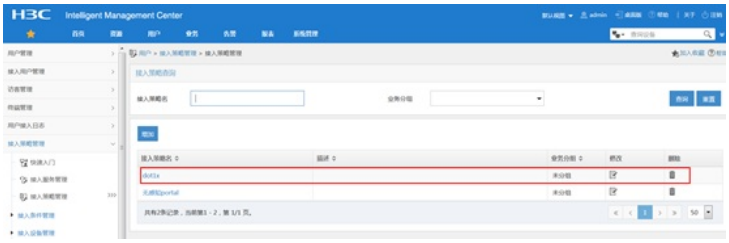


图6 成功添加接入策略dot1x



#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

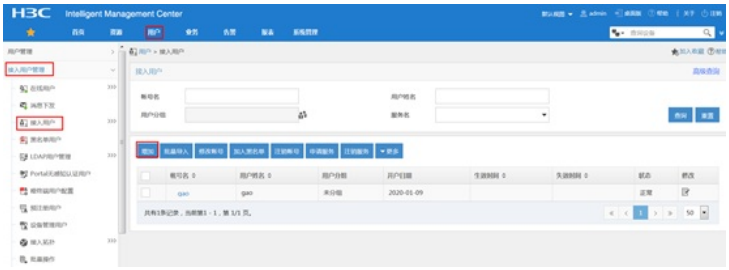


图10 添加用户dot1x

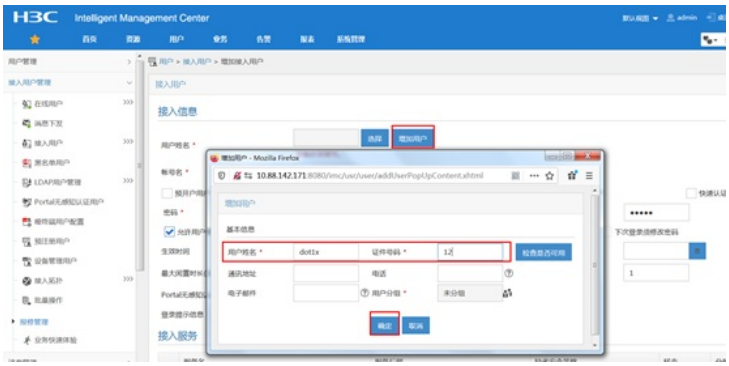


图11 增加接入用户界面

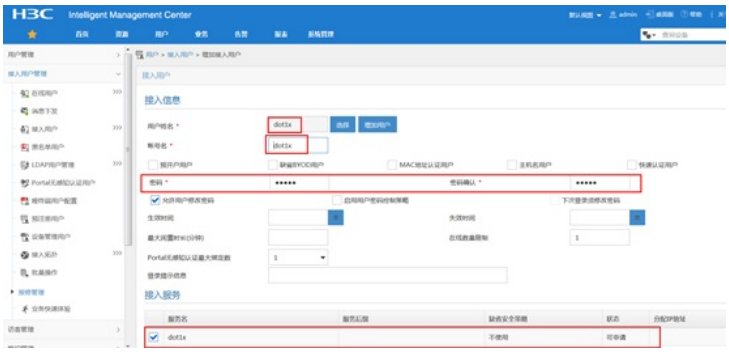


图12 创建接入用户dot1x成功

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

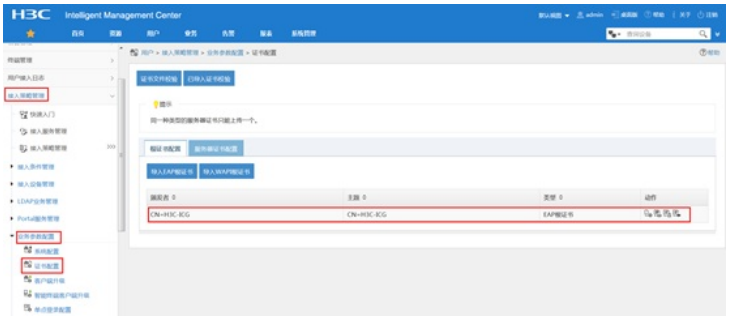
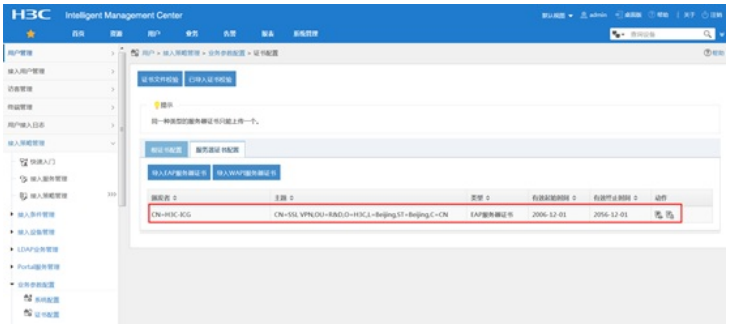


图14 导入EAP服务器证书

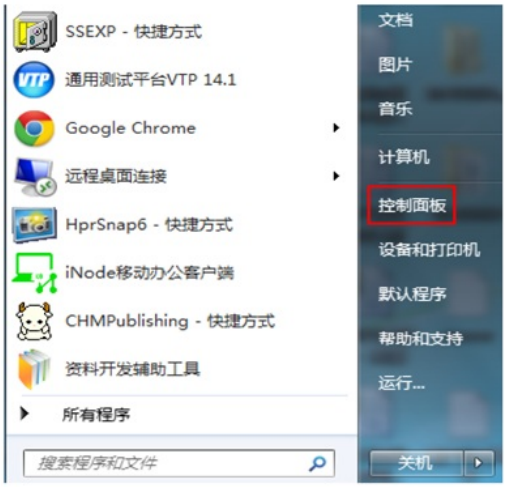


1.2 配置客户端

配置无线网卡

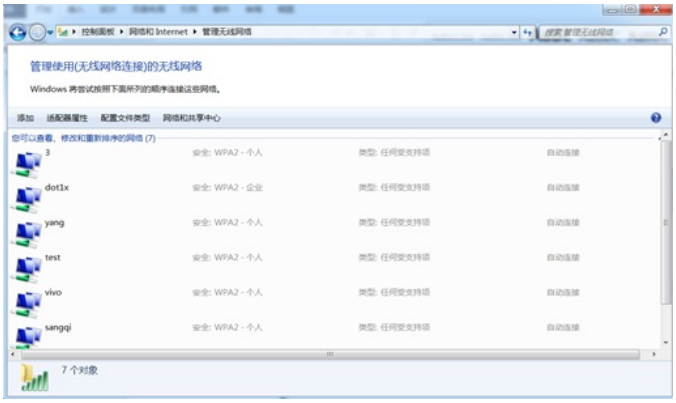
·下面以Windows 7为例，说明无线网卡的配置。

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)”。

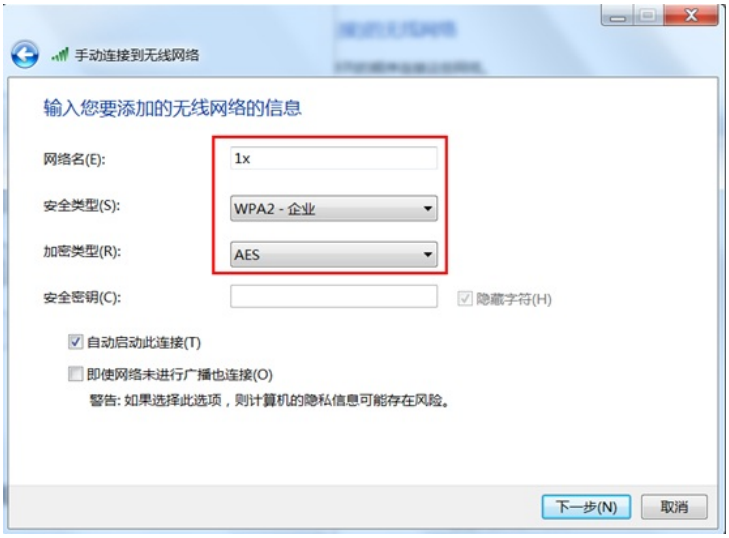
添加无线网络信息。

·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。

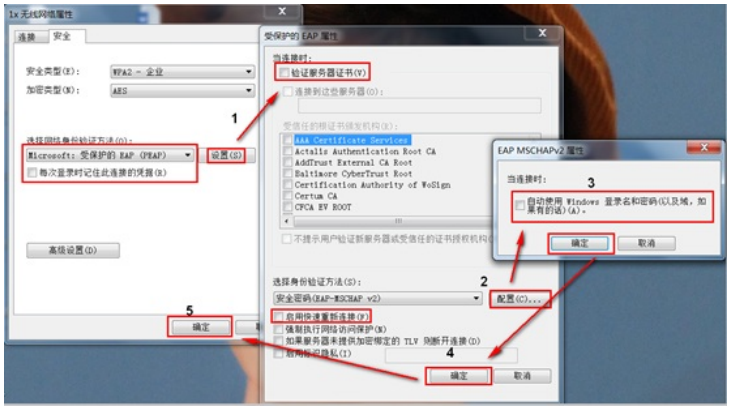
· 去掉“验证服务器证书(V)”前复选框中的勾；

·去掉“启用快速重新连接”前复选框中的勾；

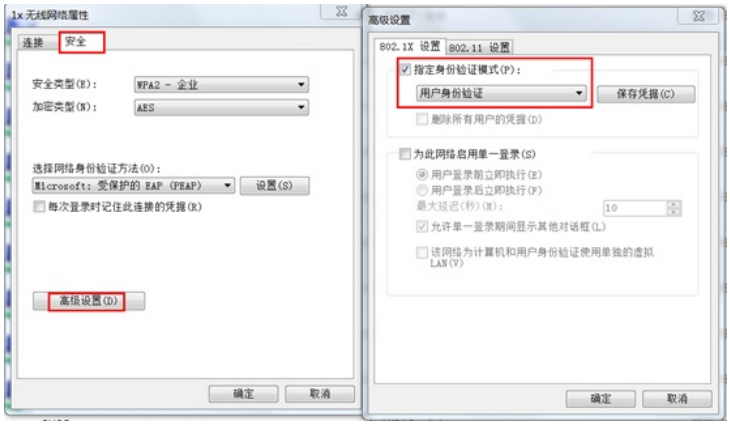
·单击“选择身份验证方法(S)”后面的<配置>按钮；

·在弹出的“EAP MSCHAPv2属性”对话框中，去掉复选框中的勾；

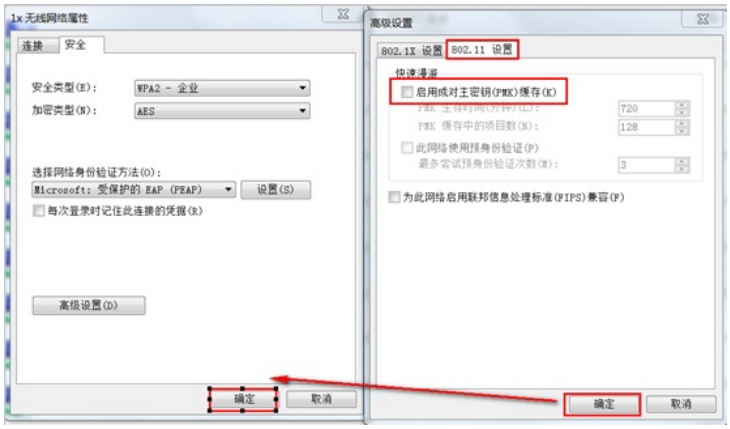
· 然后单击<确定>按钮，返回“受保护的EAP属性”界面，再单击<确定>按钮。



#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”。

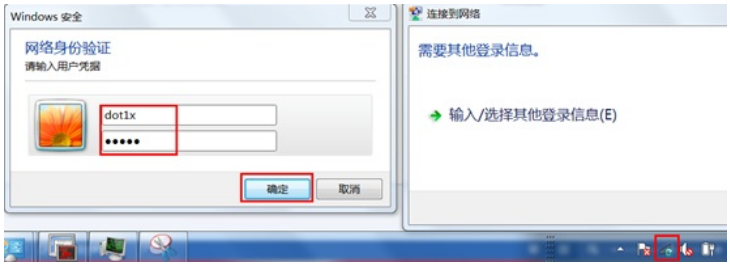


单击“802.11设置”页签，去掉“启用成对主密钥(PMK)缓存”前的复选框中的勾，然后单击<确定>按钮。



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

display wlan client

Total number of clients: 1

MAC address User name AP name R IP address VLAN

e4b3-1899-4436 dot1x ap10 1 192.168.39.2 39

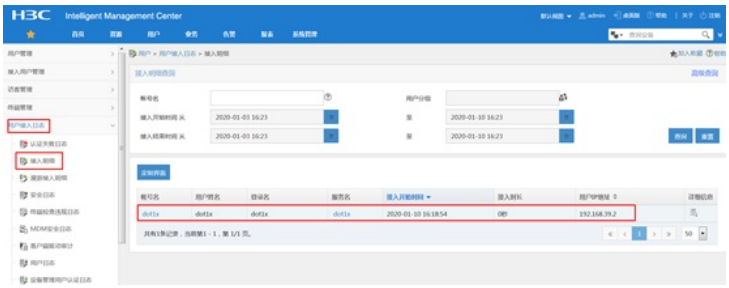
dis wlan client verbose
Total number of clients: 1

MAC address : e4b3-1899-4436
IPv4 address : 192.168.39.2
IPv6 address : N/A
Username : dot1x
AID : 2
AP ID : 81
AP name : ap10
Radio ID : 1
SSID : 1x
BSSID : 542b-de99-5760
VLAN ID : 39
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 : Supported
STBC TX capability : Supported
LDPC RX capability : Not supported
SU beamformee capability : 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
NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Supported HT MCS set : 0, 1, 2, 3, 4, 5, 6, 7,
8, 9, 10, 11, 12, 13, 14,
15
Supported rates : 6, 9, 12, 18, 24, 36,
48, 54 Mbps
QoS mode : WMM
Listen interval : 250
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 19seconds
FT status : Inactive

dis dot1x connection
Total connections: 1
User MAC address : e4b3-1899-4436
AP name : ap10
Radio ID : 1
SSID : 1x
BSSID : 542b-de99-5760
Username : dot1x

Authentication domain : 1x
IPv4 address : 192.168.39.2
Authentication method : EAP
Initial VLAN : 39
Authorization VLAN : 39
Authorization ACL number : N/A
Authorization user profile : N/A
Termination action : Default
Session timeout period : 86401 s
Online from : 2020/01/10 14:41:18
Online duration : 0h 0m 26s

在服务器侧同时能查看到用户上线信息



配置关键点

无