H3C无线控制器EAD认证典型配置举例(V7)

wlan接入 802.1X AAA 李晨光 2016-07-06 发表

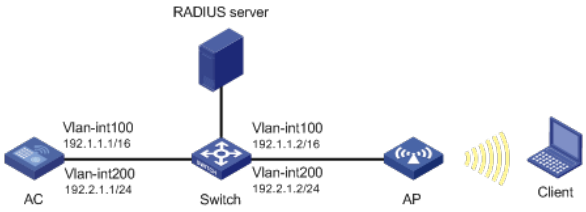
本文档介绍EAD认证的典型配置举例。

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接入和EAD认证相关特性。

如图3-1所示，Switch作为DHCP服务器为AP和Client分配IP地址。现要求在AC上配置EAD认证，使客户端通过该认证才可以接入无线网络。



1.1 配置步骤

1.1.1 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。

system-view

[AC] vlan 100

[AC-vlan100] quit

[AC] interface vlan-interface 100

[AC-Vlan-interface100] ip address 192.1.1.1 16

[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 192.2.1.1 24

[AC-Vlan-interface200] quit

配置AC和Switch相连侧的接口GigabitEthernet1/0/1为Trunk类型，禁止VLAN 1报文通过，允许VLAN 100和VLAN 200通过，当前Trunk口的PVID为100。

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] port link-type trunk

[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1

[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200

[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100

[AC-GigabitEthernet1/0/1] quit

(2) 开启端口安全功能，并配置802.1X认证方式为eap。

[AC] port-security enable

[AC] dot1x authentication-method eap

(3) 配置认证策略

创建名为radius1的RADIUS方案并进入其视图。

[AC] radius scheme radius1

设置主认证RADIUS服务器的IP地址8.1.1.16。

[AC-radius-radius1] primary authentication 8.1.1.16

设置主计费RADIUS服务器的IP地址8.1.1.16。

[AC-radius-radius1] primary accounting 8.1.1.16

配置认证报文的共享密钥为明文example。

[AC-radius-radius1] key authentication simple example
配置计费报文的共享密钥为明文example。
[AC-radius-radius1] key accounting simple example
配置实时计费的时间间隔为3分钟。
[AC-radius-radius1] timer realtime-accounting 3
配置设备发送RADIUS报文使用的源IP地址为192.1.1.1。
[AC-radius-radius1] nas-ip 192.1.1.1

(4) 配置认证域

配置认证域为radius1。
[AC] domain radius1
配置lan-access用户使用RADIUS方案radius1进行认证、授权和计费。
[AC-isp-radius1] authentication lan-access radius-scheme radius1
[AC-isp-radius1] authorization lan-access radius-scheme radius1
[AC-isp-radius1] accounting lan-access radius-scheme radius1

(5) 配置ACL

创建一个序号为3000的IPv4高级ACL，并进入其视图。
[AC] acl advanced 3000
定义一条规则，允许IP报文通过。
[AC-acl-ipv4-adv-3000] rule permit ip
[AC-acl-ipv4-adv-3000] quit
创建一个序号为3001的IPv4高级ACL，并进入其视图。
[AC] acl advanced 3001
定义一条规则，允许UDP报文通过。
[AC-acl-ipv4-adv-3001] rule permit udp
定义一条规则，禁止TCP报文通过。
[AC-acl-ipv4-adv-3001] rule deny tcp
[AC-acl-ipv4-adv-3001] quit

(6) 配置无线服务

创建无线服务模板1，并进入无线服务模板视图。
[AC] wlan service-template 1
配置SSID为service。
[AC-wlan-st-1] ssid service
配置无线客户端上线后将被加入到VLAN 200。
[AC-wlan-st-1] vlan 200
配置身份认证与密钥管理的模式为802.1X。
[AC-wlan-st-1] akm mode dot1x
配置加密套件为CCMP，安全信息元素为RSN。
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
配置用户接入认证模式为802.1X。
[AC-wlan-st-1] client-security authentication-mode dot1x
配置dot1x认证的domain域为radius1
[AC-wlan-st-1] dot1x domain radius1
使能无线服务模板。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit

(7) 配置AP

创建手工AP，名称为officeap，型号名称为WA4320i-ACN。
[AC] wlan ap officeap model WA4320i-ACN
设置AP的序列号为210235A1K6C15A003025。
[AC-wlan-ap-officeap] serial-id 210235A1K6C15A003025
进入AP的Radio 2视图，并将无线服务模板1绑定到Radio 2上。
[AC-wlan-ap-officeap] radio 2
[AC-wlan-ap-officeap-radio-2] service-template 1
开启Radio 2的射频功能。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit

(8) 配置AC到RADIUS服务器的静态路由

[AC] ip route-static 8.0.0.0 8 192.2.1.2

1.1.2 配置Switch

(1) 配置Switch的接口

创建VLAN 100及其对应接口，并为该接口配置IP地址，用于转发AC和AP间CAPWAP隧道内的流量。

system-view

[Switch] vlan 100

[Switch-vlan100] quit

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ip address 192.1.1.2 16

[Switch-Vlan-interface100] quit

创建VLAN 200及其对应接口，并为该接口配置IP地址，用于转发Client无线报文。

[Switch] vlan 200

[Switch-vlan200] quit

[Switch] interface vlan-interface 200

[Switch-Vlan-interface200] ip address 192.2.1.2 24

[Switch-Vlan-interface200] quit

创建VLAN 8及其对应接口，并为该接口配置IP地址，用于与RADIUS服务器通信。

[Switch] vlan 8

[Switch-vlan8] quit

[Switch] interface vlan-interface 8

[Switch-Vlan-interface8] ip address 8.1.1.2 8

[Switch-Vlan-interface8] quit

配置Switch和AC相连侧的接口GigabitEthernet1/0/1为Trunk类型，禁止VLAN 1报文通过，允许VLAN 100和VLAN 200通过，当前Trunk口的PVID为100。

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] port link-type trunk

[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1

[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200

[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100

[Switch-GigabitEthernet1/0/1] quit

配置Switch与AP相连侧的GigabitEthernet1/0/2为trunk类型，禁止VLAN 1报文通过，允许VLAN 100和VLAN 200通过，并设置PVID为VLAN100。

[Switch] interface gigabitethernet 1/0/2

[Switch-GigabitEthernet1/0/2] port link-type trunk

[Switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1

[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200

[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100

开启Switch和AP相连的接口GigabitEthernet1/0/2的PoE供电功能。

[Switch-GigabitEthernet1/0/2] poe enable

[Switch-GigabitEthernet1/0/2] quit

配置Swith与Radius service相连侧的GigabitEthernet1/0/3为trunk类型, 禁止VLAN 1报文通过，允许VLAN 100和VLAN 200通过，并设置PVID为VLAN 8。

[Switch] interface gigabitethernet 1/0/3

[Switch-GigabitEthernet1/0/3] port link-type trunk

[Switch-GigabitEthernet1/0/3] undo port trunk permit vlan 1

[Switch-GigabitEthernet1/0/3] port trunk permit vlan 100 200

[Switch-GigabitEthernet1/0/3] port trunk pvid vlan 8

(2) 配置DHCP服务

开启DHCP功能。

[Switch] dhcp enable

创建名为vlan100的DHCP地址池，配置地址池动态分配的网段为192.1.0.0/16，地址池中不参与自动分配的IP地址为192.1.1.1，网关地址为192.1.1.2，为AP分配IP地址。

[Switch] dhcp server ip-pool vlan100

[Switch-dhcp-pool-vlan100] network 192.1.0.0 mask 255.255.255.0

[Switch-dhcp-pool-vlan100] forbidden-ip 192.1.1.1

[Switch-dhcp-pool-vlan100] gateway-list 192.1.1.2

[Switch-dhcp-pool-vlan100] quit

创建名为vlan200的DHCP地址池，配置地址池动态分配的网段为192.2.1.0/24，地址池中不参与自动分配的IP地址为192.2.1.1，网关地址为192.2.1.2，为Client分配IP地址。

[Switch] dhcpserverip-pool vlan200

[Switch-dhcp-pool-vlan200] network 192.2.1.0 mask 255.255.255.0

[Switch-dhcp-pool-vlan200] forbidden-ip 192.2.1.1

[Switch-dhcp-pool-vlan200] gateway-list 192.2.1.2

[Switch-dhcp-pool-vlan200] quit

1.1.3 配置RADIUSservice（iMC V7）

- 下面以iMC为例（使用iMC版本为：iMC PLAT 7.2、iMC EAD 7.2），说明RADIUS server的基本配置。
- 在服务器上已经完成证书的安装。

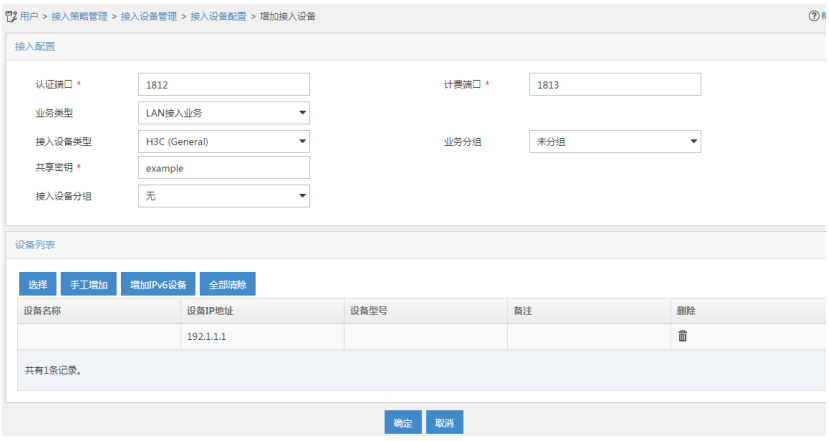
1. 在iMC上配置MAC认证项

接入设备配置：

(1) 在iMC“用户>接入策略管理>接入设备管理”中选择“接入设备配置”页面，在“接入设备配置”页面中单击<增加>按钮，增加接入设备。

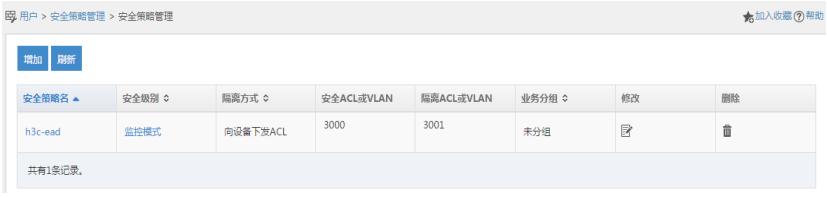
(2) 在弹出的“增加接入设备”页面中：

- 设置认证、计费共享密钥为example，其它保持缺省配置；
- 手工增加接入设备，添加IP地址为192.1.1.1的接入设备；
- 点击<确定>按钮，完成接入设备的添加。



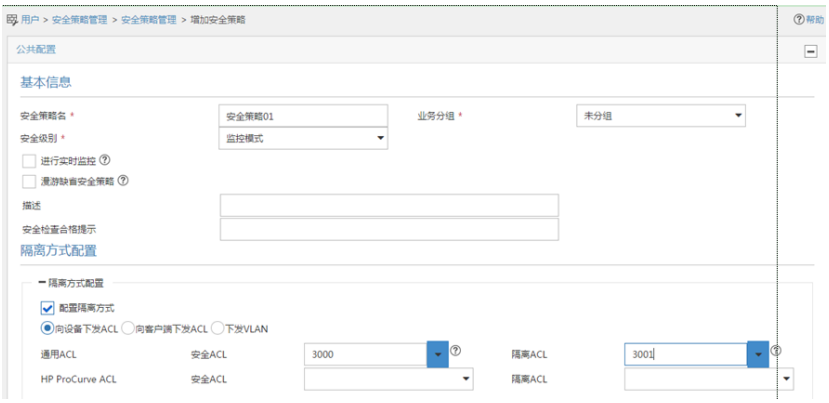
2. 配置安全策略

(1) 在iMC“用户>安全策略管理”中选择“安全策略管理”，在“安全策略管理”页面中单击<增加>按钮，增加安全策略。



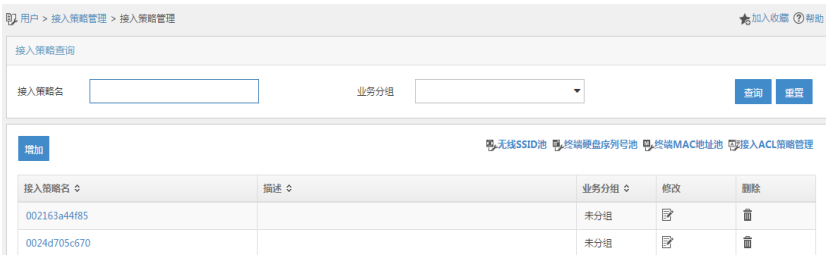
(2) 在弹出的“增加安全策略”页面中：

- 配置安全策略名为“安全策略01”；安全级别选择“监控模式”；
- 配置隔离方式为“向设备下发ACL”，并设置安全ACL为3000，隔离ACL为3001；
- 点击<确定>按钮，完成安全策略的添加。



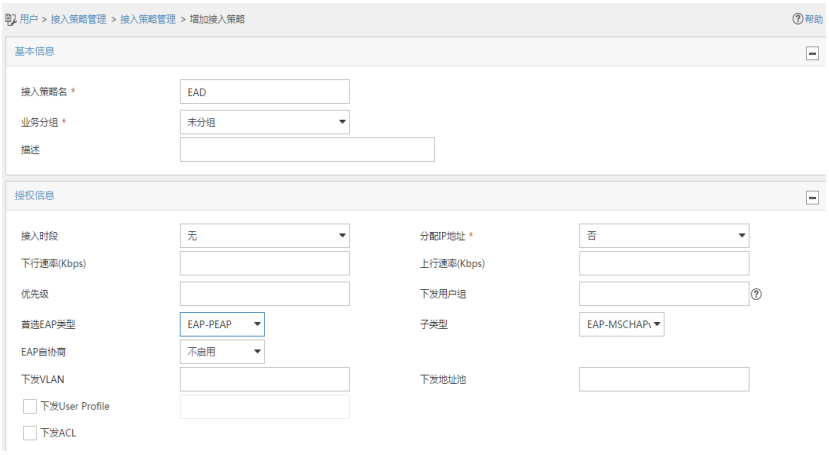
3. 配置接入策略

(1) 在iMC“用户>接入策略管理”中选择“接入策略管理”，在“接入策略管理”页面中单击<增加>按钮，增加接入服务配置。



(2) 在弹出的“增加接入策略”页面中：

- 配置接入策略名为EAD；
- 选择首选EAD类型为EAP-PEAP认证，子类型为EAP-MSCHAPv2；
- 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，其它配置采用缺省值；
- 点击<确定>按钮，完成接入策略的添加。

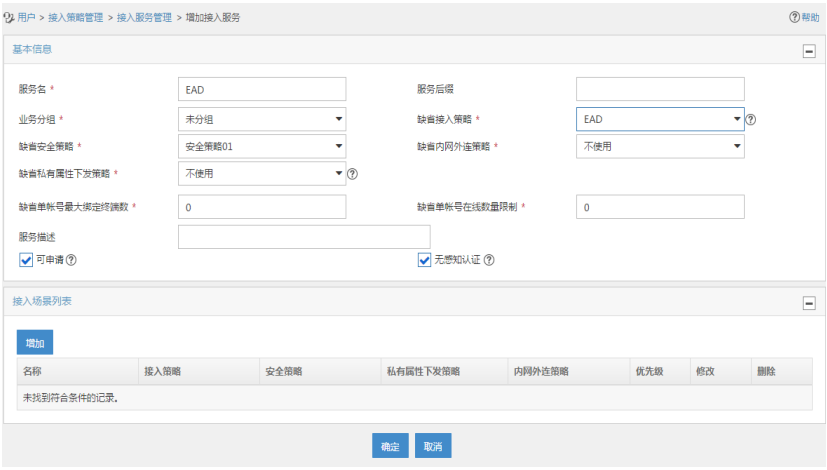


4. 配置服务策略

(1) 在iMC“用户>接入策略管理”中选择“接入服务管理”，在“接入服务管理”页面中单击<增加>按钮，增加接入服务配置。

(2) 在弹出的“增加接入服务”页面中，

- 配置服务名为EAD；
- 缺省安全策略选择安全策略01；
- 缺省接入策略为EAD，其它配置采用缺省值；
- 点击<确定>按钮，完成服务配置。

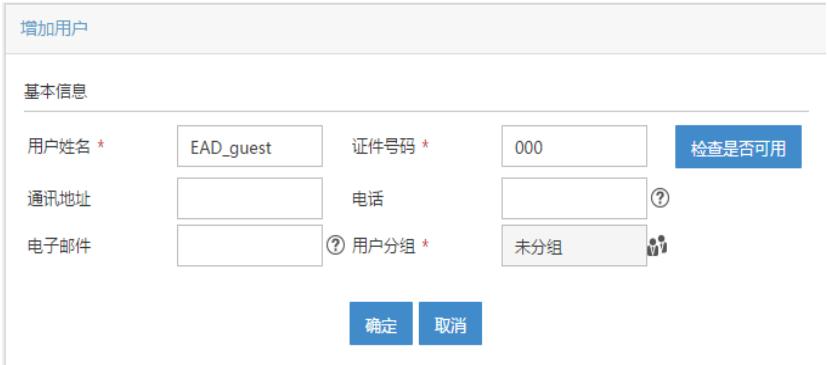


5. 配置帐号用户：

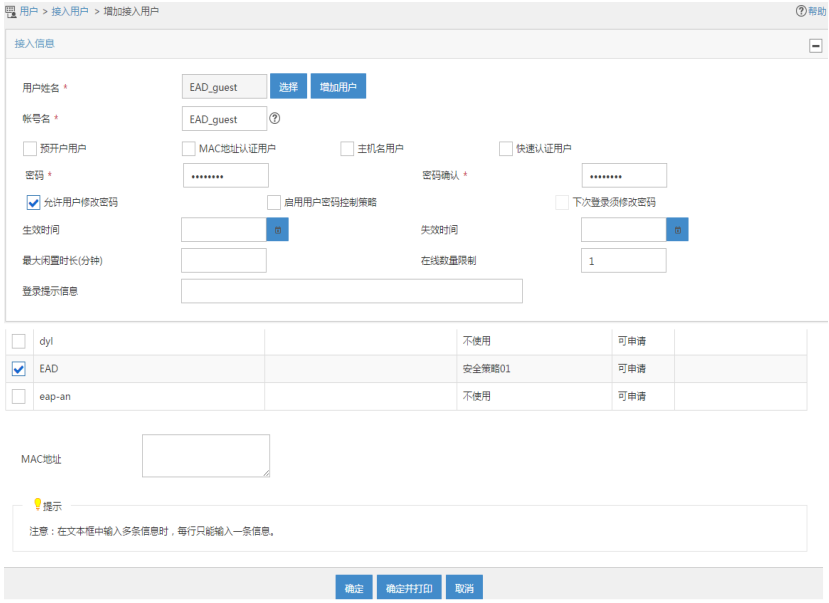
(1) 在iMC“用户>接入用户”页面中单击<增加>按钮，增加接入用户。

(2) 在增加接入用户界面，单击<增加用户>。

(3) 在弹出增加用户窗体中输入用户名为“EAD_guest”，证件号码可以根据需要输入相关证件号码，然后点击<确定>按钮，提示增加用户成功，并返回增加接入用户界面。



(4) 页面输入帐号和密码（这里采用的用户名为EAD_guest，密码为12345678），选择前面配置的接入服务为EAD，其它参数可以根据需要配置，然后点击<确定>按钮，完成配置。



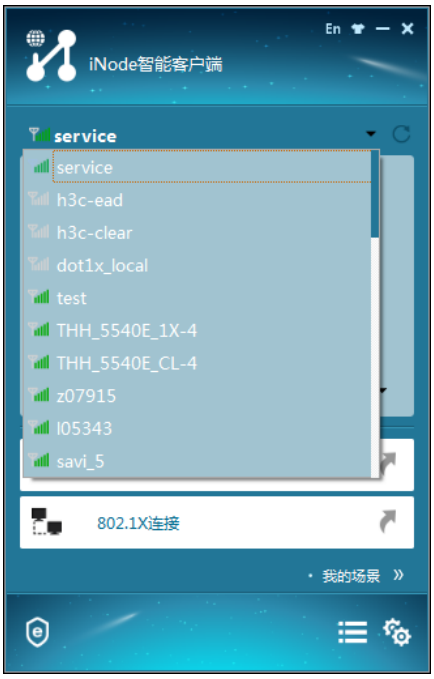
1.1.4 iNode客户端配置

iNode客户端配置如下所示：

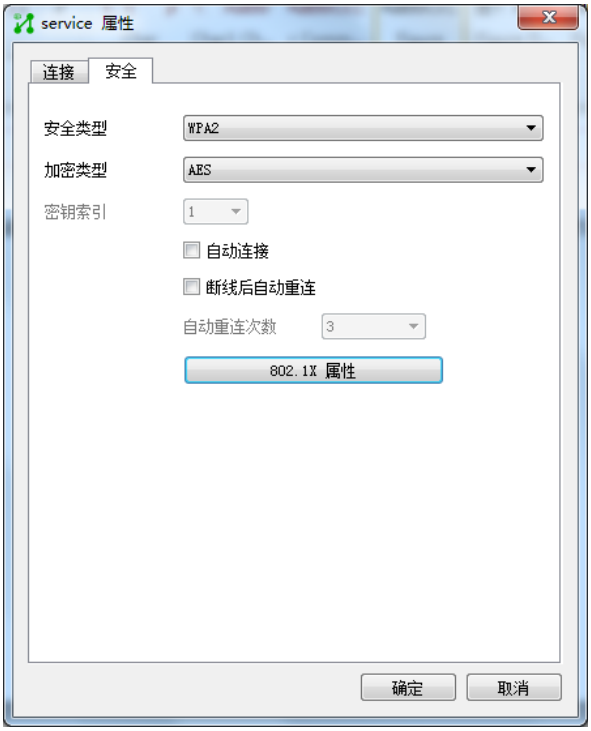
(1) 打开iNode客户端。

(2) 点击无线连接，出现无线连接界面。

(3) 点击无线连接窗体右侧的倒三角，选择配置的SSID为service的无线服务。

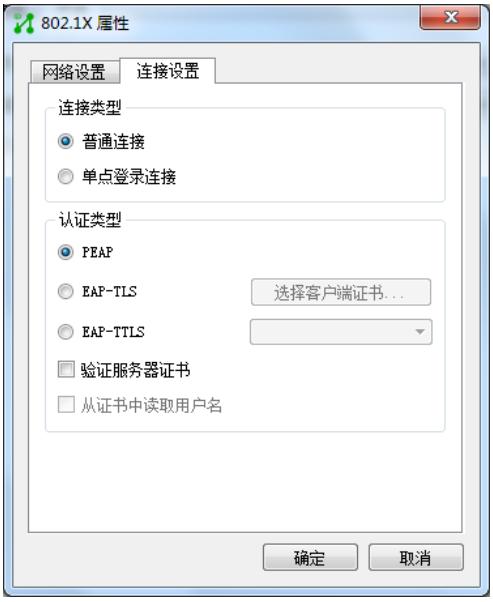


(4) 点击连接右侧的倒三角，选择属性。在属性对话框中选择“安全”页面，选择安全类型为WPA2，加密类型为AES，然后点击“802.1x属性”。



(5) 在802.1X属性对话框中选择“网络设置”，报文类型为“多播”，其他选项采用默认值，点击<确定>。

(6) 在“802.1X属性”窗体中选择“连接设置”，认证类型为“PEAP”，其他选项不动，然后点击确定。



(7) 关闭属性窗体后，返回iNode无线连接界面，输入用户名为EAD_guest，密码为12345678。

(9) 点击连接，连接成功后如下。

1.2 验证配置

(1) 使用**display dot1x sessions**查看dot1x用户已在线。

```
display dot1x sessions
AP name: officeap Radio ID: 2  SSID: service
  Online 802.1X users: 1
      MAC address       Auth state
      0015-00bf-e84d    Authenticated
```

(2) 使用**display wlan client verbose**查看EAD是否下发，查看到ACL3000，由此可知EAD安全策略下发成功

```
display wlan client verbose
Total number of clients: 1

 MAC address                  : 0015-00bf-e84d
 IPv4 address                 : 192.2.1.3
 IPv6 address                 : N/A
 Username                     : ead_guest
 AID                          : 1
 AP ID                        : 2
 AP name                      : officeap
 Radio ID                     : 2
 SSID                         : service
 BSSID                        : 3891-d58a-8930
 VLAN ID                      : 200
 Sleep count                  : 18
 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           : Not supported
 LDPC RX capability           : Not supported
 SU beamformee capability     : Not supported
 MU beamformee capability     : Not supported
 Beamformee STS capability    : N/A
 Block Ack                    : TID 0  Out
```

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 : 34
Rx/Tx rate : 58.5/324
Authentication method : Open system
Security mode : RSN
AKM mode : 802.1X
Cipher suite : CCMP
User authentication mode : 802.1X
Authorization ACL ID : 3000
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 2minutes 49seconds
FT status : Inactive

1.3 配置文件

- AC

```
#
 dot1x authentication-method eap
#
 port-security enable
#
vlan 100
#
vlan 200
#
wlan service-template 1
 ssid service
 vlan 200
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain radius1
 service-template enable
#
interface Vlan-interface100
 ip address 192.1.1.1 255.255.0.0
#
interface Vlan-interface200
 ip address 192.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 port trunk pvid vlan 100
#
 ip route-static 8.0.0.0 8 192.2.1.2
```

```
#
acl advanced 3000
 rule 0 permit ip
#
acl advanced 3001
 rule 0 permit udp
 rule 5 deny tcp
#
radius scheme radius1
 primary authentication 8.1.1.16
 primary accounting 8.1.1.16
 key authentication cipher $c$3$YCjREST8/BuXrsEKyY9nY8QQfmrN3w==
 key accounting cipher $c$3$yPGJYnF7FE+/36JrXfn+DYGq/8ngZA==
 timer realtime-accounting 3
 nas-ip 192.1.1.1
#
domain radius1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
wlan ap officeap model WA4320i-ACN
 serial-id 210235A1K6C15A003025
 radio2
  radio enable
  service-template 1
#
        ·        Switch
#
 dhcp enable
#
vlan8
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
 gateway-list 192.1.1.2
 network 192.1.0.0 mask 255.255.0.0
 forbidden-ip 192.1.1.1
#
dhcp server ip-pool vlan200
 gateway-list 192.2.1.2
 network 192.2.1.0 mask 255.255.255.0
 forbidden-ip 192.2.1.1
#
interface Vlan-interface8
 ip address 8.1.1.2 255.0.0.0
#
interface Vlan-interface100
 ip address 192.1.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 192.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
```

```
 port trunk permit vlan 100 200
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 port trunk pvid vlan 100
 poe enable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 port trunk pvid vlan 8
#
```

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。