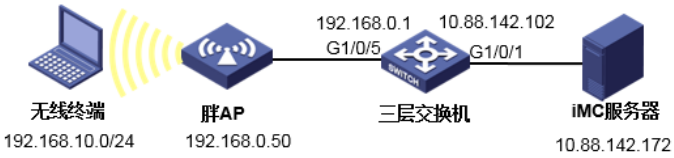
胖AP结合远程radius服务器做802.1X认证的典型配置

802.1X AAA 杨海严 2017-08-05 发表

在胖AP上开启802.1X，无线终端802.1X认证接入网络，认证服务器为iMC服务器。



无线终端属于vlan10，使用192.168.10.0/24网段地址，网关192.168.10.1在胖AP上；胖AP使用vlan-interface1（地址为192.168.0.50）与三层交换机互联；iMC服务器的地址为10.88.142.172。

（1）胖AP配置

```
#和三层交换机互联地址
interface Vlan-interface1
 ip address 192.168.0.50 255.255.255.0
#缺省路由，下一跳指向三层交换机
 ip route-static 0.0.0.0 0.0.0.0 192.168.0.1
#
vlan 10
#无线终端业务网关
interface Vlan-interface10
 ip address 192.168.10.1 255.255.255.0
#无线终端dhcp地址池，分配192.168.10.0/24网段、网关地址和dns
dhcp server ip-pool vlan10
 network 192.168.10.0 mask 255.255.255.0
 gateway-list 192.168.10.1
 dns-list 114.114.114.114
#dhcp禁止分配网关地址
 dhcp server forbidden-ip 192.168.10.1
#使能dhcp
 dhcp enable

#使能端口安全
 port-security enable
#802.1x认证方式为eap
 dot1x authentication-method eap
#配置radius方案，指定认证（授权）、计费服务器地址和密钥
radius scheme yanghaiyan
 server-type extended
 primary authentication 10.88.142.172
 primary accounting 10.88.142.172
 key authentication simple 123456
 key accounting simple 123456
 user-name-format without-domain
 nas-ip 192.168.0.50
#配置域，调用radius方案
domain yanghaiyan
 authentication lan-access radius-scheme yanghaiyan
 authorization lan-access radius-scheme yanghaiyan
 accounting lan-access radius-scheme yanghaiyan

#配置无线BSS接口为hybrid口，pvid设置为业务vlan10，untagged业务vlan10，端口模式设置为userlo
gin-secure-ext，强制认证域，关闭802.1X握手和组播触发
interface WLAN-BSS10
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 untagged
 port hybrid pvid vlan 10
```

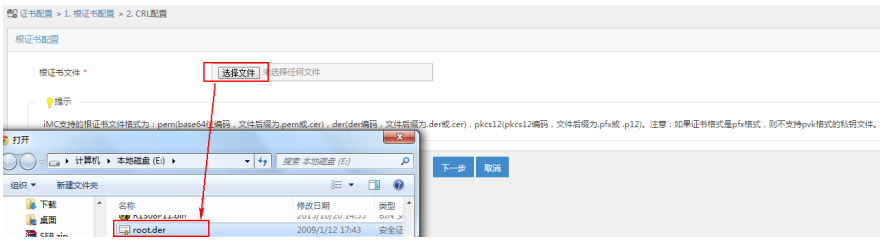
```
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
  dot1x mandatory-domain yanghaiyan
  undo dot1x handshake
 undo dot1x multicast-trigger
#新建加密类型的无线服务模板，配置ssid、加密套件和安全ie
wlan service-template 10 crypto
 ssid yhy_fat-ap_imc-1x
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#radio下服务模板和BSS接口绑定
interface WLAN-Radio1/0/2
 service-template 10 interface wlan-bss 10
```

（2）三层交换机配置

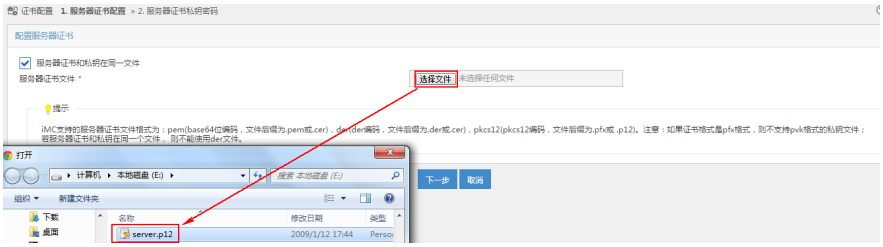
```
#和iMC服务器互联地址
interface Vlan-interface1
 ip address 10.88.142.102 255.255.255.0
#连接iMC服务器接口
interface GigabitEthernet1/0/1
#
vlan 50
#和AP互联地址
interface Vlan-interface50
 ip address 192.168.0.1 255.255.255.0
#连接AP接口
interface GigabitEthernet1/0/5
 port access vlan 50
 poe enable
#无线终端网段的回程路由，下一跳指向AP
ip route-static 192.168.10.0 24 192.168.0.50
```

（3）iMC服务器配置

#导入根证书

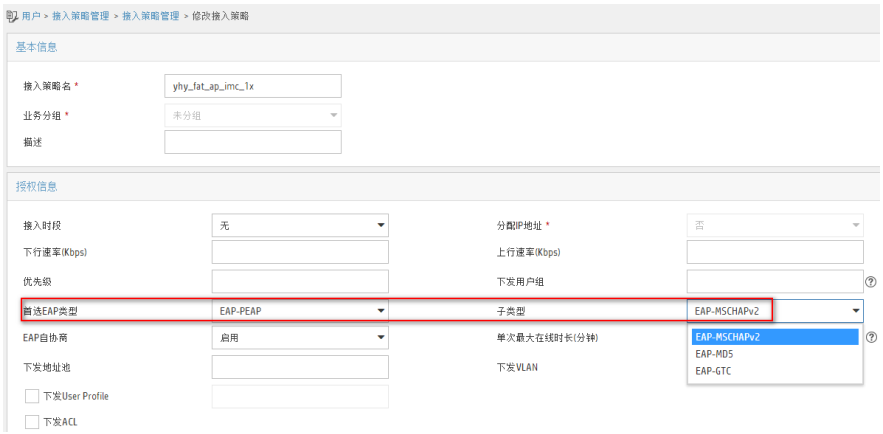


#导入服务器证书，注意要输入私钥密码

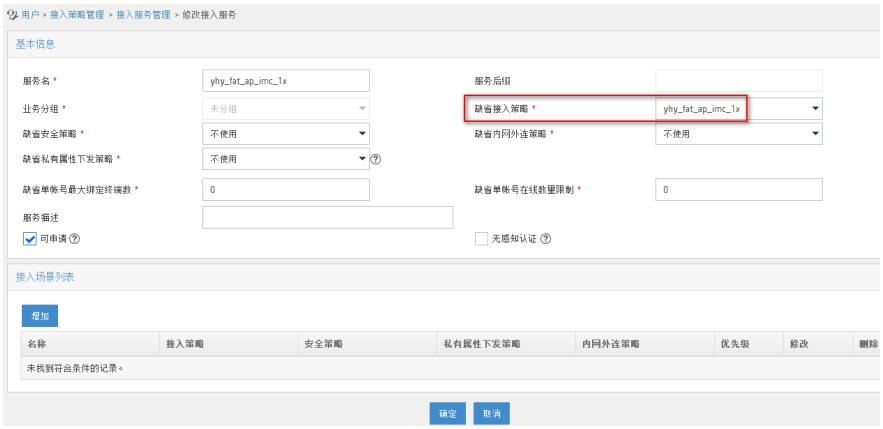


#增加接入设备，注意业务类型为“LAN接入业务”，密码要正确，以AP的管理地址（192.168.0.50）增加到设备列表

#增加接入策略，首选EAP类型选择“EAP-PEAP”，子类型为“EAP-MSCHAPv2”



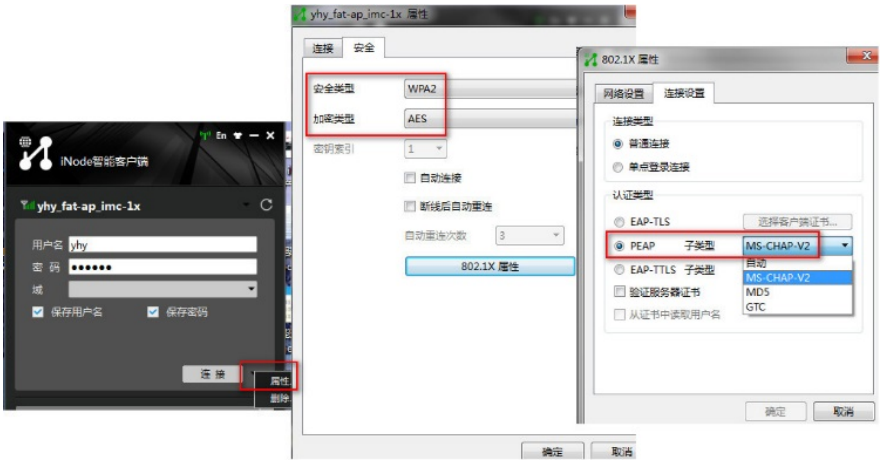
#增加接入服务，调用接入策略



#增加接入用户，配置账号密码，调用接入服务

（4）测试

#打开iNode客户端，安全类型选WPA2，加密类型AES，选PEAP 子类型MS-CHAPV2

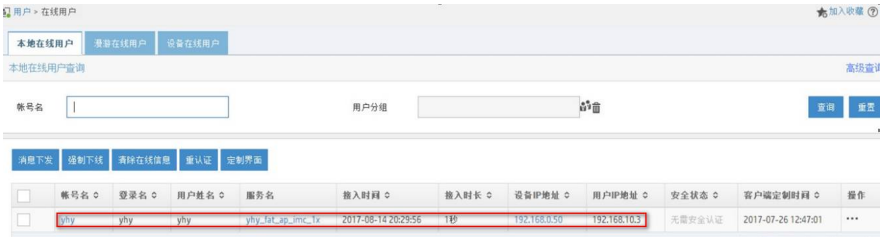


#输入账号密码，认证成功

#认证通过后，无线终端和iMC服务器连通性正常

```
PING: 传输失败。General failure.
请求超时。
来自 10.88.142.172 的回复: 字节=32 时间=4ms TTL=126
来自 10.88.142.172 的回复: 字节=32 时间=2ms TTL=126
来自 10.88.142.172 的回复: 字节=32 时间=2ms TTL=126
来自 10.88.142.172 的回复: 字节=32 时间=2ms TTL=126
来自 10.88.142.172 的回复: 字节=32 时间=2ms TTL=126
来自 10.88.142.172 的回复: 字节=32 时间=40ms TTL=126
来自 10.88.142.172 的回复: 字节=32 时间=4ms TTL=126
来自 10.88.142.172 的回复: 字节=32 时间=2ms TTL=126
```

#iMC服务器上查看用户已经在线



#查看终端在线表项

<WA2620i-AGN>display wlan client

Total Number of Clients : 1

Client Information

SSID: yhy_fat-ap_imc-1x

MAC Address User Name APID/RID IP Address VLAN

6480-99e9-3478 bTNZG... 1 /2 192.168.10.3 10

#查看终端详细信息

<WA2620i-AGN>dis wlan client verbose

Total Number of Clients : 1

Client Information

MAC Address : 6480-99e9-3478

User Name : b2cJHRgDMXQtSx1jJ1F+fQJPZcM= yhy

AID : 1

Radio Interface : WLAN-Radio1/0/2

SSID : yhy_fat-ap_imc-1x

BSSID : 70f9-6daf-ee10

Port : WLAN-BSS10

VLAN : 10

……

RSSI : 36

Rx/Tx Rate : 65/144.4

Client Type : WPA2(RSN)

Authentication Method : Open System

Authentication Mode : Central

AKM Method : Dot1X

4-Way Handshake State : PTKINITDONE

Group Key State : IDLE

Encryption Cipher : AES-CCMP

……

（1）无线终端、胖AP、三层交换机和iMC服务器是跨三层组网的，要注意配置路由，否则可能导致认证失败或者业务不通。

（2）导入的根证书和服务器证书一定要是配套的，另外注意iMC服务器的系统时间要正确，否则可能导致证书导入失败。

（3）iMC服务器上接入策略和iNode客户端参数最好保持一致，否则可能导致认证不上。