WX系列AC本地802.1X认证（EAP-PEAP方式）功能的配置

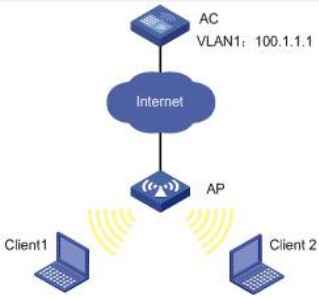
802.1X AAA wlan接入 宋斌 2011-08-31 发表

WX系列AC本地802.1X认证（EAP-PEAP方式）功能的配置

一、 组网需求：

WX系列AC、FIT AP、便携机（安装有无线网卡）

二、 组网图：



三、 特性介绍：

本特性在WLAN NAS设备上支持本地对无线用户进行认证的功能。对于组网中不支持EAP认证的AAA Server，本特性通过实现EAP OffLoad功能，使NAS设备作为STA与AAA Server的桥梁，帮助二者顺畅的完成认证过程。

本特性提供了对WLAN接入用户的本地认证功能，支持MD5，EAP_TLS，EAP_MSCHAPv2，EAP_PEAP多种认证方式，使得用户可以自如的根据需要灵活配置各种安全限制，同时不需要布置AAA服务器，减小了网络拓扑图的复杂度。

四、 配置信息：

```
#
 sysname H3C
#
 domain default enable system
#
 telnet server enable
#
 port-security enable
#
                dot1x              authentication-method              eap

#
vlan 1
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
pki entity auth
  common-name local-auth
  organization h3c-auth
#
pki domain local
  certificate request entity auth
  crl check disable
#
dhcp server ip-pool zlb
 network 100.1.1.0 mask 255.255.255.0
 gateway-list 100.1.1.1
#
user-group system
```

```
 user-group eap
 #
 local-user admin
  password simple admin
  authorization-attribute level 3
  service-type telnet
 local-user eap
  password simple eap
  group eap
  service-type lan-access
 #
 wlan rrm
  dot11a mandatory-rate 6 12 24
  dot11a supported-rate 9 18 36 48 54
  dot11b mandatory-rate 1 2
  dot11b supported-rate 5.5 11
  dot11g mandatory-rate 1 2 5.5 11
  dot11g supported-rate 6 9 12 18 24 36 48 54
 #
 wlan service-template 1 crypto
  ssid h3c-wpa
  bind WLAN-ESS 1
  cipher-suite tkip
  security-ie wpa
  service-template enable
 #
 ssl server-policy 1
  pki-domain local
  ciphersuite rsa_rc4_128_sha
  handshake timeout 180
  close-mode wait
  session  cachesize 1000
 #
 eap-profile eap1
  ssl-server-policy 1
  method peap-mschapv2
 #
 interface NULL0
 #
 interface Vlan-interface1
  ip address 100.1.1.1 255.255.255.0
 #
 interface M-GigabitEthernet2/0/0
 #
 interface Ten-GigabitEthernet2/0/1
 #
 interface WLAN-ESS1
  port-security port-mode userlogin-secure-ext
  port-security tx-key-type 11key
  undo dot1x handshake
 #
 wlan ap ap1_002 model WA2210-AG
  serial-id 210235A29D0083000778
  radio 1
   channel 1
   service-template 1
   radio enable
 #
  dhcp enable
 #
  local-server authentication eap-profile eap1
 #
  load xml-configuration
 #
```

```
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
#
return
```

五、 主要配置步骤：

配置WLAN服务，在无线口配置端口安全模式为dot1x方式

```
#
wlan service-template 1 crypto
 ssid eap
 bind WLAN-ESS 1
 cipher-suite tkip
 security-ie wpa
 service-template enable
#

#
interface WLAN-ESS1
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
#
```

＃配置dot1x认证为eap方式，并使能端口安全；

```
[AC]dot1x authentication-method eap
[AC]port-security enable
```

＃配置PKI参数

```
#
pki entity auth
  common-name local-auth
  organization h3c-auth
#
pki domain local
  certificate request entity auth
  crl check disable
#
```

＃导入证书；

如果之前已经导入过证书，需要先销毁公共密钥，才能再进行证书导入：

```
[AC]public-key local destroy rsa
Local key pair is in use by local certificate of domain "local" ,Do you want to delete lo
cal certificate first? [Y/N]:y
```

导入根证书：

```
[AC]pki import-certificate ca domain local der filename certnew.cer
The trusted CA's finger print is:
    MD5  fingerprint:5710 DE77 4771 641F 5C38 8CF4 25DE 9CAA
    SHA1 fingerprint:02AB BAB7 F8CC 6D1E 3EF8 5EAB 5FBD B448 A8FE 24FA

Is the finger print correct?(Y/N):y

Import CA certificate successfully.
%Oct 17 17:02:33:554 2008 H3C PKI/4/Verify_CA_Root_Cert:CA root certificate of t
he domain local is trusted.
[H3C]
%Oct 17 17:02:33:563 2008 H3C PKI/4/Update_CA_Cert:Update CA certificates of t
he Domain local successfully.
%Oct 17 17:02:33:572 2008 H3C PKI/4/Import_CA_Cert:Import CA certificates of
the domain local successfully.
```

导入Server SSL证书：

```
[AC] pki import-certificate local domain local p12 filename server_ssl.pfx
```

Please input challenge password:
Import local certificate successfully.
%Oct 17 17:06:26:777 2008 H3C PKI/4/Verify_Cert:Verify certificate CN=pt_web of the domain local successfully.
Import key pair successfully.
%Oct 17 17:06:26:783 2008 H3C PKI/4/Import_Local_Cert:Import local certificate of the domain local successfully.
[H3C]
%Oct 17 17:06:26:838 2008 H3C PKI/4/Import_Local_Key:Import local private key of the domain local successfully.
[AC]

配置SSL服务策略；

```
#
ssl server-policy 1
 pki-domain local
 ciphersuite rsa_rc4_128_sha
 handshake timeout 180
 close-mode wait
 session  cachesize 1000
#
```

配置本地认证方式为eap-peap，并使能本地认证服务；

```
[AC]eap-profile eap1
[AC-eap-prof-eap]method peap-mschapv2
[AC-eap-prof-eap]ssl-server-policy 1
[AC-eap-prof-eap]quit
[AC]local-server authentication eap-profile eap1
```

创建用户组

```
[AC]user-group eap
```

创建本地用户，服务类型为lan-access；

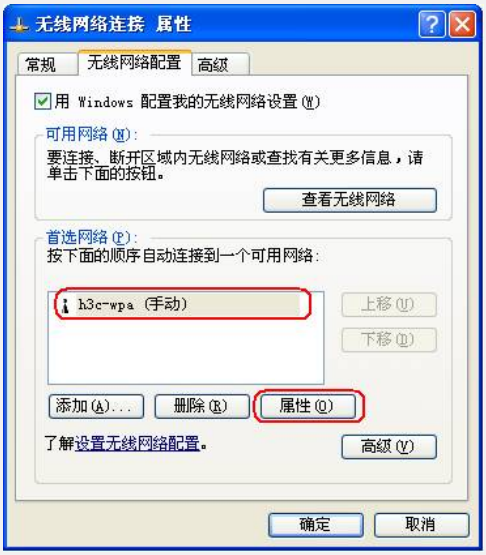
```
#
local-user eap
 password simple eap
 group eap
 service-type lan-access
#
```

六、 结果验证：

本例使用Windows无线客户端进行验证：

1、在Windows无线客户端中，通过“刷新网络列表”搜索相应的SSID，本例中的SSID为h3c-wpa，然后选择“更改高级设置”，如下图所示：

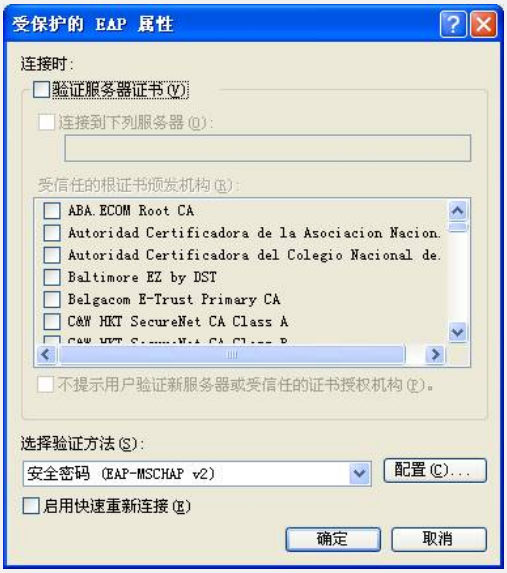
2、在弹出的对话框中，选择“无线网络配置”，在“首选网络”中选择“h3c-wpa”，然后点击“属性”，如下图所示：



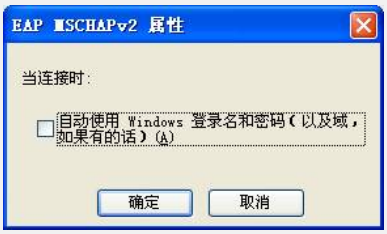
3、在弹出的“h3c-wpa属性”对话框中，在“关联”项中根据SSID的配置，在“网络验证 (A)”中选择“WPA”，在“数据加密 (D)”中选择“TKIP”，如下图所示：

4、选择“验证”项，在“EAP类型 (T)”中选择“受保护的EAP (PEAP)”，然后点击“属性”，如下图所示：

5、在弹出的“受保护的EAP属性”的对话框中，如需验证服务器证书，在“验证服务器证书 (V)”选项上打勾，否则勾掉该选项。然后点击“配置”，本例中不验证服务器证书，如下图所示：



6、在弹出的“EAP　MSCHAPv2 属性”对话框中，勾掉“自动使用Windows登录名和密码”选项，然后选择“确定”。



7、按照以上步骤设置完成后，选择连接SSID　h3c-wpa，对弹出的对话框中输入用户名111和密码111，如下图所示：

8、认证通过后，SSID　h3c-wpa上会出现“已连接上”，并且客户端可正常访问网络，如下图所示：


无线网络连接
网络任务
刷新网络列表
为家庭或小型办公室设置无线网络
相关任务
了解无线网络
更改首选网络的顺序
更改高级设置
选择无线网络
单击以下列表中的项目以连接到区域内的无线网络或获得更多信息(M)。
h3c-wpa
已连接上
启用安全的无线网络 (WPA)
brcmwap-psk
启用安全的无线网络 (WPA)
h3c
未设置安全机制的无线网络
NTU-BJ-OFFICE
启用安全的无线网络 (WPA2)
h3c-web
未设置安全机制的无线网络
断开(D)