胖AP实现本地802.1x认证（加密模式）

wlan接入 802.1X 裴锐霖 2016-02-01 发表

一、需求说明

在没有radius服务器，只有一台胖ap，需实现本地加密的dot1x认证。如果在AC上实现本地dot1x认证，则需要导入证书。而在胖AP上实现dot1x认证，则有两种，一种是不加密的dot1x认证，需要结合iNode配合实现（请看案例“WA1208E与iNode客户端配合实现本地802.1x认证功能的典型配置”）。本文的需求是加密的dot1x认证，且不需要iNode客户端配合，和正常的dot1x认证功能一样。

二、版本设备要求

版本要求：version 5.20, Release 1308以上。一般室内型AP都支持

三、WX交换机的典型配置

```
#
version 5.20, Release 1308P11
#
sysname ap3
#
domain default enable system
#
ipv6
#
telnet server enable
#
port-security enable  //开启端口安全
#
dot1x authentication-method eap  //配置为eap方式
#
password-recovery enable
#
vlan 1
#
vlan 2
#
domain lynn  //配置认证域为本地方式
authentication lan-access local
authorization lan-access local
accounting lan-access local
access-limit disable
state active
idle-cut disable
self-service-url disable
domain system
access-limit disable
state active
idle-cut disable
self-service-url disable
#
dhcp server ip-pool vlan1
network 192.168.1.0 mask 255.255.255.0
gateway-list 192.168.1.1
#
dhcp server ip-pool vlan2
network 192.168.2.0 mask 255.255.255.0
gateway-list 192.168.2.1
#
user-group system
group-attribute allow-guest
#
```

local-user admin
password cipher c3$nmBMe/uKDpkC4Xtv6LT2J3xYJ3SGLsvl8nrT
service-type lan-access //配置dot1x认证的用户
#
wlan rrm
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 clear
ssid lynn
service-template enable
#
wlan service-template 2 crypto
ssid dot1x
cipher-suite ccmp
security-ie rsn
service-template enable
#
ssl server-policy lynn //配置ssl策略
#
eap-profile lynn //配置eap-profile并且调用ssl策略
ssl-server-policy lynn
method md5
method peap-mschapv2
#
interface NULL0
#
interface Vlan-interface1
ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface2
ip address 192.168.2.1 255.255.255.0
#
interface Ethernet1/0/1
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3
#
interface WLAN-BSS1
#
interface WLAN-BSS2 //按照规范配置dot1x认证端口
port link-type hybrid
port hybrid vlan 1 to 2 untagged
port hybrid pvid vlan 2
port-security port-mode userlogin-secure-ext
port-security tx-key-type 11key
undo dot1x handshake
dot1x mandatory-domain lynn
undo dot1x multicast-trigger
#
interface WLAN-BSS32
#
interface WLAN-Radio1/0/1
channel 6
service-template 1 interface wlan-bss 1
service-template 2 interface wlan-bss 2
#
dhcp enable
#
undo gratuitous-arp-learning enable
#

local-server authentication eap-profile lynn //本地认证服务器

#

load xml-configuration

#

load tr069-configuration

#

user-interface con 0

user-interface vty 0 4

authentication-mode none

user privilege level 3

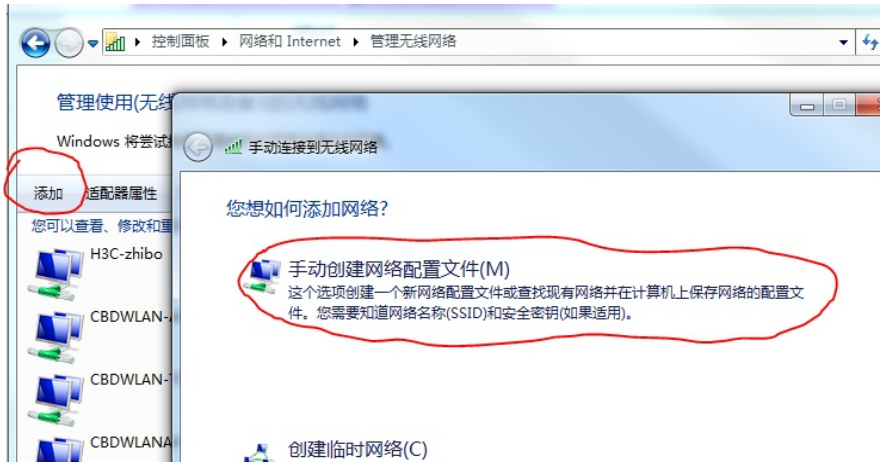
set authentication password cipher c3$oRgCQ4ZZjy5ErcWGwzfdc3IxMn1KyRja23i6NHQ=

#

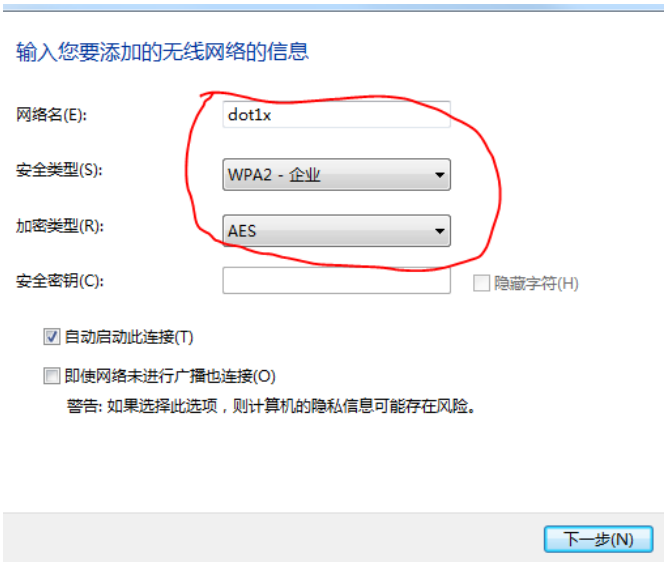
return

四、客户端配置

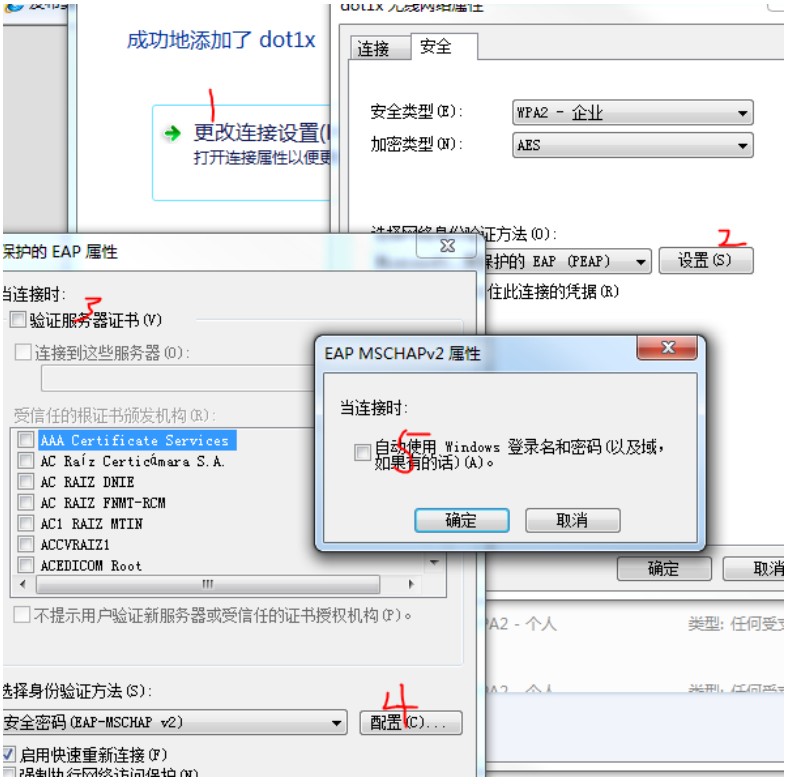
1、手动添加ssid



2、设置加密方式



3、设置不需要验证服务器证书和不需要Windows登录名和密码



4、连接无线，输入用户名和密码


```
port-security enable  //开启端口安全
#
dot1x authentication-method eap   //配置为eap方式
#
domain lynn                              //配置认证域为本地方式
authentication lan-access local
authorization lan-access local
accounting lan-access local
#
local-user admin
password cipher $c$3$nmBMe/uKDpkC4Xtv6LT2J3xYJ3SGLsvI8nrT
service-type lan-access            //配置dot1x认证的用户
#
```

ssl server-policy lynn　　//配置ssl策略
#
eap-profile lynn　　//配置eap-profile并且调用ssl策略
ssl-server-policy lynn
method md5
method peap-mschapv2
#
interface WLAN-BSS2　　//按照规范配置dot1x认证端口
port link-type hybrid
port hybrid vlan 1 to 2 untagged
port hybrid pvid vlan 2
port-security port-mode userlogin-secure-ext
port-security tx-key-type 11key
undo dot1x handshake
dot1x mandatory-domain lynn
undo dot1x multicast-trigger
#
local-server authentication eap-profile lynn　//本地认证服务器
配置完成后，在ap的根目录下会自动生成证书。