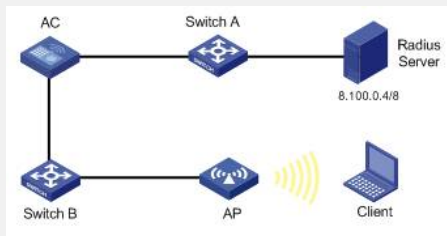


H3C WX系列AC 动态WEP典型配置

一、组网需求

无线控制器 (AC)、无线接入点 (FIT AP)、二层交换机、Radius服务器 (iMC)、无线笔记本;

二、组网图



本次配置举例中使用AC为WX5004, FIT AP为WA2620i-AGN, AC作为DHCP服务器, AP在AC上自动获取IP地址,并在AC上注册成功;笔记本终端接入无线网络 (SSID: dweptest), 在AC上获取IP地址。

三、特性介绍

WEP (Wired Equivalent Privacy, 有线等效加密) 用来保护WLAN中的授权用户所交换的数据的机密性,防止这些数据被随机窃听。WEP使用RC4加密算法 (一种流加密算法) 实现数据报文的加密保护。根据WEP密钥的生成方式, WEP加密分为静态WEP加密和动态WEP加密。

静态WEP加密要求手工指定WEP密钥,接入同一SSID下的所有无线客户端使用相同的WEP密钥。如果WEP密钥被破解或泄漏,攻击者就能获取所有密文。因此静态WEP加密存在比较大的安全隐患。并且手工定期更新WEP密钥会给网络管理员带来很大的设备管理负担。

动态WEP加密的自动密钥管理机制对原有的静态WEP加密进行了较大的改善。在动态WEP加密机制中,用来加密单播数据帧的WEP密钥并不是手工指定的,而是由无线客户端和服务器通过802.1X协议协商产生,这样每个无线客户端协商出来的WEP单播密钥都是不同的,提高了单播数据帧传输的安全性。动态WEP加密配合802.1X使用,在提供了用户身份认证的同时,也实现了对传输数据的安全保护。

四、主要配置步骤

配置VLAN接口及其IP地址。

```
[AC]vlan 10
[AC-vlan10]quit
[AC]interface Vlan-interface 10
[AC-Vlan-interface10]ip address 100.10.1.54 255.255.0.0
[AC-Vlan-interface10]quit
[AC]interface Vlan-interface 1
[AC-Vlan-interface1]ip address 100.1.1.54 255.255.0.0
[AC-Vlan-interface1]quit
# 配置GE1/0/1和GE1/0/2加入VLAN。
[AC]interface GigabitEthernet 1/0/1
[AC-GigabitEthernet1/0/1]port hybrid vlan 1 to 10 tagged
[AC-GigabitEthernet1/0/1]quit
[AC]interface GigabitEthernet 1/0/2
[AC-GigabitEthernet1/0/2]port hybrid vlan 1 to 10 tagged
[AC-GigabitEthernet1/0/2]quit
# 配置到Radius服务器的静态路由。
[AC]ip route-static 0.0.0.0 0 100.1.1.254
# 配置认证域
[AC]radius scheme leap
[AC-radius-leap]primary authentication 8.100.0.4 key testkey
[AC-radius-leap]primary accounting 8.100.0.4 key cipher testkey
[AC-radius-leap]quit
[AC]domain acs
[AC-isp-acs]authentication default radius-scheme leap
[AC-isp-acs]authorization default radius-scheme leap
[AC-isp-acs]accounting default radius-scheme leap
# 开启端口安全,配置EAP认证方式
```

```

[AC] port-security enable
[AC] dot1x authentication-method eap
# 配置WLAN-ESS接口
[AC]interface WLAN-ESS10
[AC-WLAN-ESS10]port link-type hybrid
[AC-WLAN-ESS10]mac-vlan enable
# 配置端口安全为dot1x方式
[AC-WLAN-ESS10]port-security port-mode userlogin-secure-ext
[AC-WLAN-ESS10]undo dot1x handshake
[AC-WLAN-ESS10]undo dot1x multicast-trigger
[AC-WLAN-ESS10]dot1x mandatory-domain acs
[AC-WLAN-ESS10]quit
# 在AC上配置动态WEP方式加密的无线服务
[AC] wlan service-template 11 crypto
[AC-wlan-st-11]ssid dweptest
[AC-wlan-st-11]bind WLAN-ESS 10
[AC-wlan-st-11]cipher-suite wep104
[AC-wlan-st-11]wep mode dynamic
[AC-wlan-st-11]wep default-key 1 wep104 pass-phrase 1234567890123
[AC-wlan-st-11]wep key-id 1
[AC-wlan-st-11]service-template enable
# 在AC的AP视图下配置AP名称为wa2210，型号名称这里选择WA2210-AG
[AC] wlan ap wa2210 model WA2210-AG
[AC-wlan-ap-wa2210] serial-id 210235A22W0079000278
# 进入AP的radio1射频视图，配置服务模板与射频1进行关联，使能AP的radio 1射频
[AC-wlan-ap-wa2210] radio 1
[AC-wlan-ap-wa2210-radio-1] service-template 11 vlan-id 10
[AC-wlan-ap-wa2210-radio-1] radio enable

```

五、配置信息：

```

[AC]display current-configuration
#
version 5.20, Ess 2302P01
#
sysname AC
#
domain default enable system
#
port-security enable
#
dot1x authentication-method eap
#
vlan 1
#
vlan 10
#
radius scheme leap
primary authentication 8.100.0.4 key cipher r2XPFox/kW/c5Pzyb0TNTg==
primary accounting 8.100.0.4 key cipher r2XPFox/kW/c5Pzyb0TNTg==
#
domain acs
authentication default radius-scheme leap
authorization default radius-scheme leap
accounting default radius-scheme leap
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
#
user-group system
group-attribute allow-guest
#
local-user admin
password simple admin
authorization-attribute level 3

```

```

service-type telnet
service-type web
#
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 11 crypto
ssid dweptest
bind WLAN-ESS 10
cipher-suite wep104
wep mode dynamic
wep default-key 1 wep104 pass-phrase cipher O'W3[_M"$4LR[%;
wep key-id 1
service-template enable
#
interface NULL0
#
interface Vlan-interface1
ip address 100.1.1.54 255.255.0.0
#
interface Vlan-interface10
ip address 100.10.1.54 255.255.0.0
#
interface GigabitEthernet1/0/1
port link-type hybrid
port hybrid vlan 1 10 tagged
#
interface GigabitEthernet1/0/2
port link-type hybrid
port hybrid vlan 1 10 tagged
#
interface WLAN-ESS10
port link-type hybrid
port hybrid vlan 1 untagged
mac-vlan enable
port-security port-mode userlogin-secure-ext
undo dot1x handshake
dot1x mandatory-domain acs
undo dot1x multicast-trigger
#
wlan ap wa2210 model WA2210-AG
serial-id 210235A22W0079000278
radio 1
service-template 11 vlan 10
radio enable
#
ip route-static 0.0.0.0 0.0.0.0 100.1.1.254
#
undo info-center logfile enable
#
arp-snooping enable
#
load xml-configuration
#
user-interface con 0
idle-timeout 0 0
user-interface vty 0 4
authentication-mode scheme
user privilege level 3
#
return

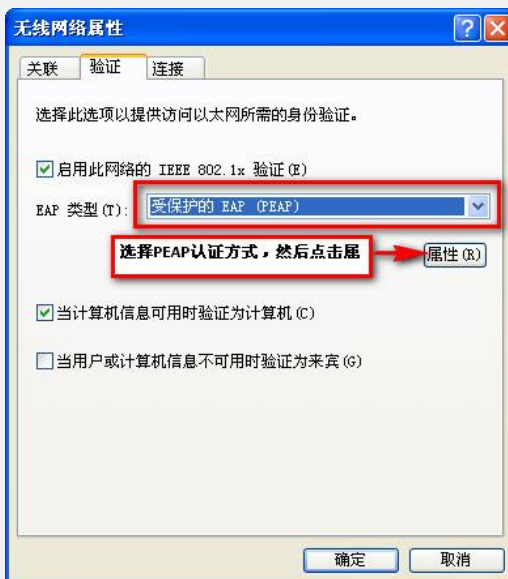
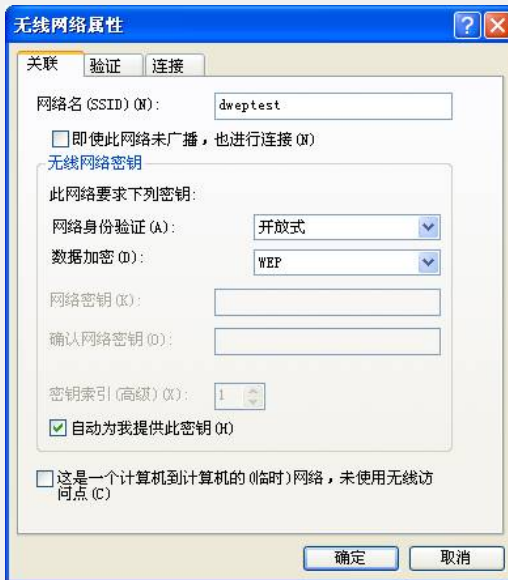
```

六、结果验证:

1、无线客户端选择动态WEP加密SSID: dweptest, 并进行802.1x认证:



2、设置终端802.1X认证方式为PEAP



3、在AC上通过命令行display connection查看用户是否认证成功。

```
[AC] display connection
Index=2848,Username=test@acs
MAC=00-1E-C1-44-47-2E
IP=100.10.47.90
IPv6=N/A
Total 1 connection(s) matched.
```

4、通过display connection ucibindex命令查看用户详细信息

```
[AC] display connection ucibindex 2848
Index=2848, Username=test@acs
MAC=00-1E-C1-44-47-2E
IP=100.10.47.90
IPv6=N/A
Access=8021X ,AuthMethod=EAP
Port Type=Wireless-802.11,Port Name=WLAN-DBSS10:2046
Initial VLAN=1, Authorization VLAN=10
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2011-05-03 10:55:28 ,Current=2011-05-03 11:05:54 ,Online=00h10m25s
Total 1 connection matched.
```