802.1x PROTOCOL ABILITY

How to test the 802.1x protocol ability
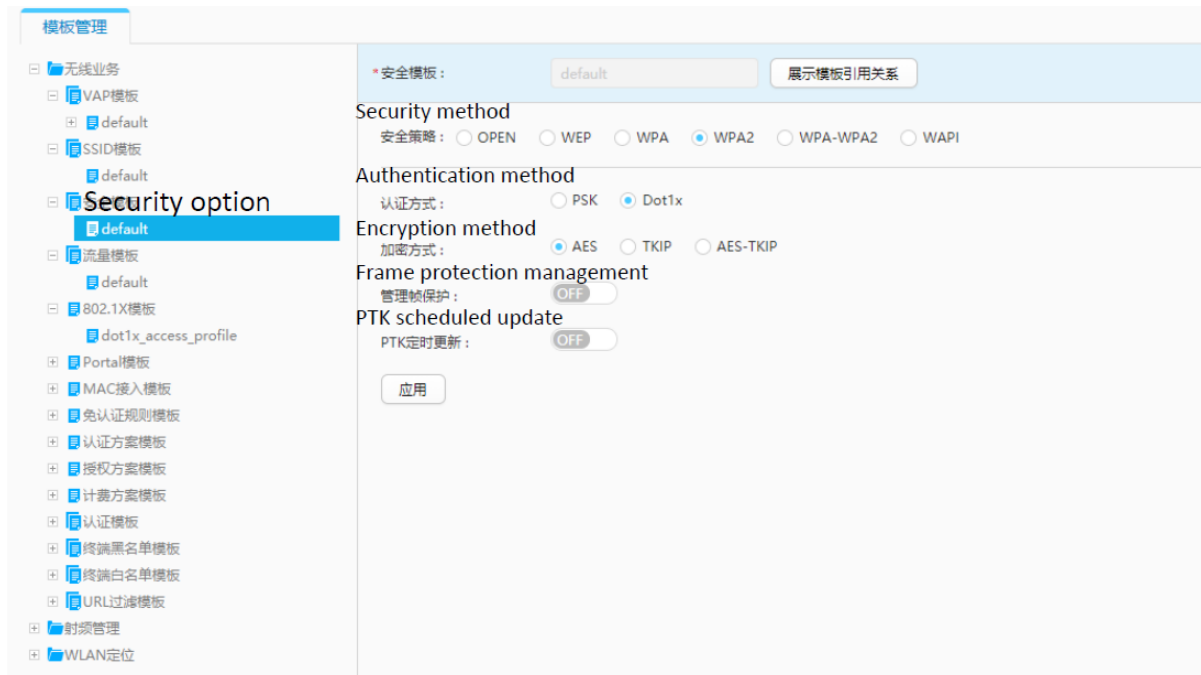
1. Router Information and configuration
Brand: Huawei
Model: AP6050DN

Main Parameters Settings：
Router interface is as follows：

The setting steps are as follows:

    sysname seewo test

\#

    http secure-server ssl-policy default_policy

        http server enable

\#

undo clock timezone

\#

ssl renegotiation-rate 1

\#

stp enable

\#

authentication-profile name default_authen_profile

authentication-profile name dot1x_authen_profile

    dot1x-access-profile dot1x_access_profile

authentication-profile name mac_authen_profile

authentication-profile name portal_authen_profile

authentication-profile name macportal_authen_profile

authentication-profile name dot1x

    dot1x-access-profile dot1x

```
            authentication-scheme server2008
            radius-server server2008
#
dns resolve
#
dhcp enable
#
dhcp server bootp
dhcp server bootp automatic
#
radius-server template default
radius-server template server2008
        radius-server shared-key
cipher %^%#h9_D"nq2CQC/')PfhS+/b{C4A8F)*"2`>31Mu-,4%^%#
        radius-server authentication 192.168.1.2 1812 weight 80
#
pki realm default
        certificate-check none
        rsa local-key-pair default
        enrollment self-signed
#
ssl policy default_policy type server
        pki-realm default
        version tls1.0 tls1.1 tls1.2
        ciphersuite rsa_aes_128_cbc_sha rsa_aes_128_sha256 rsa_aes_256_s
ha256
ssl policy https type client
        pki-realm default
        version tls1.2
        server-verify enable
        prefer-ciphersuite rsa_aes_128_sha256 rsa_aes_256_sha256
#
free-rule-template name default_free_rule
#
portal-access-profile name portal_access_profile
#
ip pool dot1x
network 192.168.1.0 mask 255.255.255.0
#
aaa
        authentication-scheme default
        authentication-scheme radius
```

```
                authentication-mode radius
        authentication-scheme server2008
                authentication-mode radius
        authorization-scheme default
        accounting-scheme default
        domain default
                authentication-scheme default
        domain default_admin
                authentication-scheme default
        local-user admin password irreversible-
cipher $1a$ln<[.2*\\I$AHD,~N7gf7#4TERR9\S+Xy7}A;Rb3T-]$tRSJj9O$
        local-user admin privilege level 15
        local-user admin service-type telnet ssh http
#
interface Vlanif1
        ip address 192.168.1.1 255.255.255.0
        dhcp select global
#
interface GigabitEthernet0/0/0
#
interface GigabitEthernet0/0/1
#
interface NULL0
#
        undo snmp-agent
#
        stelnet server enable
ssh server secure-algorithms cipher aes256_ctr aes128_ctr
ssh server secure-algorithms hmac sha2_256
ssh server key-exchange dh_group14_sha1
ssh client secure-algorithms cipher aes256_ctr aes128_ctr
ssh client secure-algorithms hmac sha2_256
ssh client key-exchange dh_group14_sha1
#
user-interface con 0
        authentication-mode password
        set authentication password cipher %^%#@}R7DhV(AXuezB@8ejIKsGMJ
(:1Kg@K}x>#:2s`Ye=9'4<'wiO(.:y0Vs,YL%^%#
user-interface vty 0 4
        authentication-mode aaa
        protocol inbound all
user-interface vty 16 20
```

```
                protocol inbound all
#
wlan
        traffic-profile name default
        security-profile name dot1x
                security wpa2 dot1x aes
        security-profile name default
                security wpa-wpa2 dot1x aes
        ssid-profile name dot1x
                ssid dot1x
        ssid-profile name default
        vap-profile name dot1x
                ssid-profile dot1x
                security-profile dot1x
                authentication-profile dot1x
        vap-profile name default
        air-scan-profile name default
        rrm-profile name default
        radio-2g-profile name default
        radio-5g-profile name default
        wids
#
interface Wlan-Radio0/0/0
        vap-profile default wlan 1
        vap-profile dot1x wlan 3
#
interface Wlan-Radio0/0/1
        vap-profile default wlan 1
        vap-profile dot1x wlan 3
#
dot1x-access-profile name dot1x_access_profile
dot1x-access-profile name dot1x
#
mac-access-profile name mac_access_profile
#
        undo ntp-service enable
#
return
```

2. Radius Server Information and configuration
PC Brand : Lenovo Thinkpad
PC Model : T440P

PC OS Version : Windows Server 2008
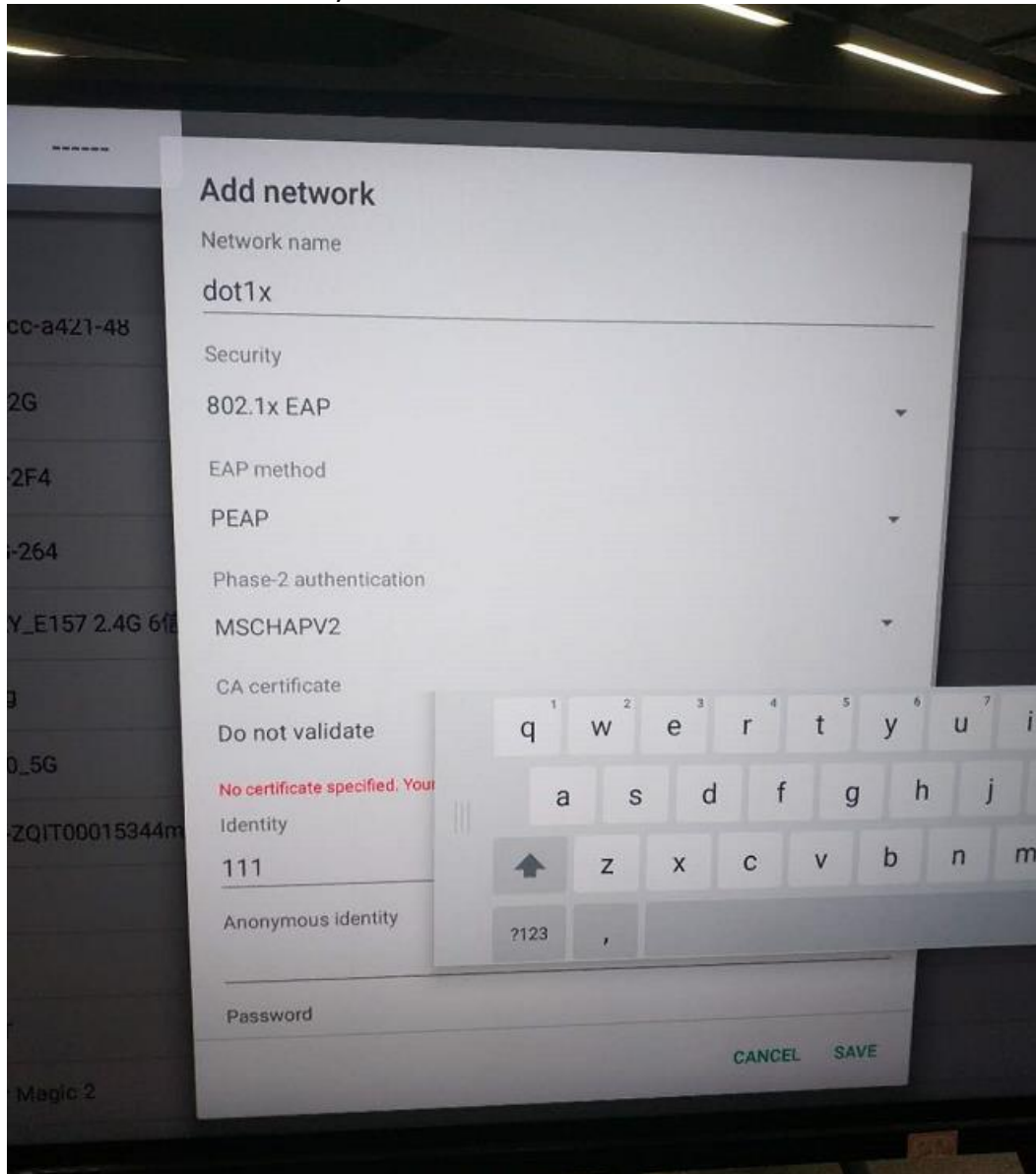
Main Parameters Settings :

See webpage :
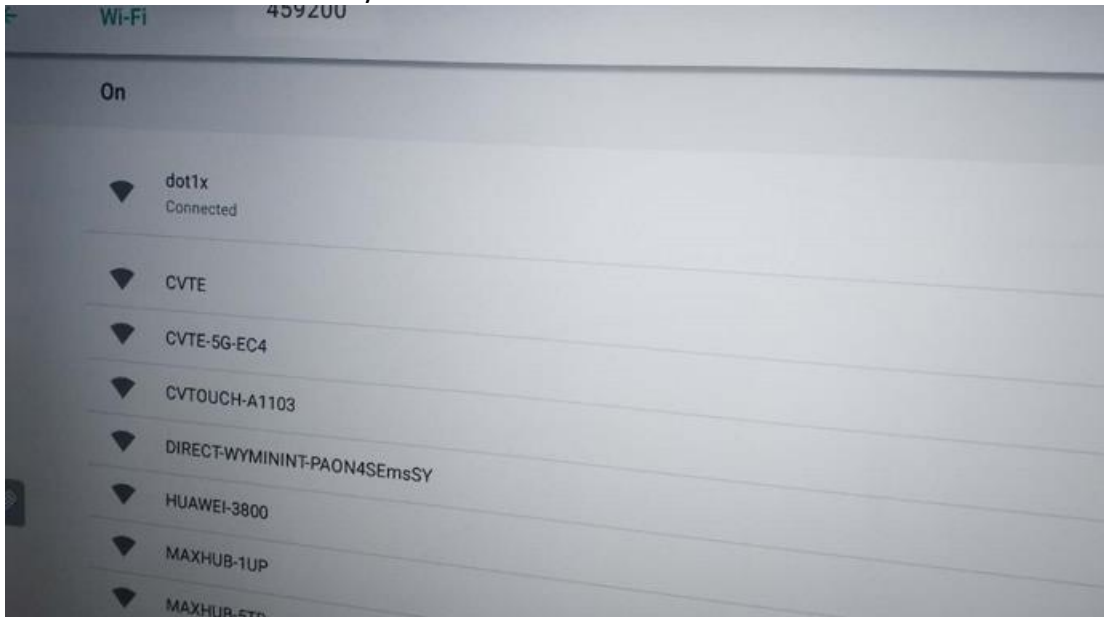https://networklessons.com/uncategorized/peap-and-eap-tls-on-server-2008-andcisco-wlc/

3. TEST RESULT

TEST RESULT: PASS

STEP1 - Add SSID manually

STEP2 - Connect successfully

STEP3 - Check the security information, and it shows 802.1x EAP