# **802.1x PROTOCOL ABILITY**

## How to test the 802.1x protocol ability

**1. Router Information and configuration** Brand: Huawei Model: AP6050DN



Connecting people with technology

#### Main Parameters Settings: Router interface is as follows:

模板管理	
	* 安全模版: default 展示模版引用关系
□ ■ VAP模板	Security method 安全策略: OPEN WEP WPA
	Authentication method
Default	Encryption method 加密方式: ● AES TKIP AES-TKIP
	Frame protection management 管理帧保护:
□ ■ 802.1X模倣 ■ dot1x_access_profile	PTK scheduled update PTK定时更新: OFF
<ul> <li>         ■ Portal横板         ■         ■ MAC接入模板         ■         ■         ■</li></ul>	应用
<ul> <li>B 总认证规则模板</li> <li>J 认证方案模板</li> </ul>	
<ul> <li>• • • • • • • • • • • • • • • • • • •</li></ul>	
<ul> <li>□ ↓ 证模板</li> <li>□ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓</li></ul>	
■ ■ 「● 終端白名単模板 ■ ■ □ UBL対波模板	
T WLANZELY	

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

## **CLEVERTOUCH®**

```
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
```

# **CLEVERTOUCH®**

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 irreversiblecipher \$1a\$In<[.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 NULLO # 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

## **CLEVERTOUCH**<sup>®</sup>

	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

# **CLEVERTOUCH**<sup>®</sup>

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

	Add network												
	Network name												
	dot1x												
-a421-48	Security										-		
	802.1x EAP												
-4	EAP method												
	PEAP									-			
54	Phase-2 authentication												
E157 2.4G 61	MSCHAPV2									•			
	CA certificate										1	7	
	Do not validate	q	1	W	е	3	r		t	у		u	i
G	No certificate specified. Your		а	S		d		f	g		h		
UT00015344m	Identity									-			
	111	4		z	х		С		v	D		n	m
	Anonymous identity	2123	,	,									
	Password												
							CAN	CEL	SA	VE			
	The second s				-								

Connecting people with technology

# **CLEVERTOUCH®**

## STEP2 - Connect successfully

Wi-F	459200	
On		
•	dot1x Connected	
	CVTE	
•	CVTE-5G-EC4	
	CVTOUCH-A1103	
	DIRECT-WYMININT-PAON4SEmesy	
	HUAWEI-3800	
	MAXHUB-1UP	
•	MAXHUR.STO	

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

dot1x 459200	
FORGET	
Signal strength	
Frequency	Excellent
Security	5 GHz
Contracts details	802. TX EAP
MAC address	
1P address	
Gateway	78:dd:d9:7e:14:7c
Subnet mask	192.168.1.192
DNS.	192.168.1.1
Unix speed	255.255.255.0
IPM Mitman	197.140
	192,108,1,1

Connecting people with technology