Client Compatibility Test Case for DellE5420 with 11ng mode

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 0.1 | 07/12/2012 | Zhonghua Xu | Initial draft |
| 0.2 | 08/11/2012 | Zhonghua Xu | Update after review on 2012-7-30 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

Glossary and Abbreviations

# Introduction

Aerohive Networks Inc. engages in testing of wireless clients to ensure compatibility with the Aerohive solution and also define best practices for that client. The purpose of this is to enable Aerohive’s Customers, partners, and resellers to have the best possible experience with Aerohive’s solution.

# Client Description

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Client Type | Client Vendor | Client Model | Client OS | OS Version | Wifi Driver | Driver Version | Wireless Mode |
| Laptop | Dell | Latitude E5420 | Win7 | Win7 Enterprise N | Intel Centrino Ultimate-N 6300 AGN | 14.0.1.2 | 802.11a/b/g/n |

# Test Objectives

The goal is to validate feature functionality on both HiveOS and HiveManager (configuration), testing shall also provide customer and negative scenarios

1. Connection rapidity between client and AP, including Probe, Auth, Association, and DHCP process.
2. Client can get authentication with its supported auth mode.
3. QoS/ WMM mechanism between client and AP with different service, such as VoIP and vedio.
4. Client can work with different power save mode
5. Capability and rapidity of client’s roaming, including different roaming methods
6. HM support to show/ log related info for client with different scenario

# Test Acceptance Criterion from Development

* Approved – MRD

N/A

* Approved – Functional Specifications

N/A

* Approved – Unit Test Plans

N/A

# Product Pass Criterion

Feature testing is considered pass when test result meets the requirement defined in the expected result field. The expected result field is defined by the requirements stated in the functional specification and/ or MRD; whichever is stricter; plus additional quality and usability expectations set by the test engineer.

# Test Bed/Topo Design

**Topo1**- Client get association with AP via wifi



**Figure01- Topo1**

**Topo2**- Client connect with AP via eth port



**Figure02- Topo2**

# Test Case with 802.11 ng Mode

Notes:

1) Auth mode is composed of Key Management, Encryption Method and Authentication Method, such as WEP/ WEP-104/ Open mode

2) In CWP auth, just test with one kind of browser on the client to verify the CWP process

3) All the cases in this chapter will be performed with 802.11ng wireless mode

## ClientComp\_DellE5420\_11ng\_Connection

### ClientComp\_DellE5420\_11ng\_Connection\_1

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Connection\_1 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Verify that client recieve probe-rsp from AP in an appropriate and timely manner. | | |
| Pre-condition | 1) Wifi0/ wifi1 is binded with an open SSID  2) Client support wifi access through wifi0/ wifi1  3) Sniffer is configured to the channel under test  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config on AP  ***AH-81b680#sh ru***  ***ssid zhxu***  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi0 ssid zhxu***  ***capwap client server name 10.155.31.201*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace table  3) Start sniffer to capture radio msg  4) Refresh SSID list on client  5) Try to associate the SSID under test  6) Stop sniffer after client get association with the AP | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  ***AH-81b680#sh log b | i itk***  ***……***  ***2012-07-13 06:48:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-13 06:48:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 45dB), level=2) step(1/6) SUCCESS***  ***……***  3) In sniffer log, there is probe-req sent from client to AP    4) In sniffer log, there is probe-rsp sent from AP after received client’s probe-req | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Connection\_2

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Connection\_2 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Verify that client recieve auth-rsp from AP in an appropriate and timely manner. | | |
| Pre-condition | 1) Wifi0/ wifi1 is binded with an open SSID  2) Client support wifi access through wifi0/ wifi1  3) Sniffer is configured to the channel under test  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace table  3) Start sniffer to capture radio msg  4) Refresh SSID list on client  5) Try to associate the SSID under test  6) Stop sniffer after client get association with the AP | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the auth-req/ auth-rsp process is correct and regular  ***AH-81b680#sh log b | i itk***  ***……***  ***2012-07-13 06:48:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-13 06:48:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 55dB), level=0) step(3/6) SUCCESS***  ***……***  3) In sniffer log, there is auth-req sent from client to AP    4) In sniffer log, there is auth-rsp sent from AP after received client’s auth-req | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Connection\_3

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Connection\_3 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Verify that client recieve association-rsp from AP in an appropriate and timely manner. | | |
| Pre-condition | 1) Wifi0/ wifi1 is binded with an open SSID  2) Client support wifi access through wifi0/ wifi1  3) Sniffer is configured to the channel under test  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace table  3) Start sniffer to capture radio msg  4) Refresh SSID list on client  5) Try to associate the SSID under test  6) Stop sniffer after client get association with the AP | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the assoc-req/ assoc-rsp process is correct and regular  ***AH-81b680#sh log b | i itk***  ***……***  ***2012-07-13 06:48:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-13 06:48:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 54dB), level=0) step(5/6) SUCCESS***  ***……***  3) In sniffer log, there is association-req sent from client to AP    4) In sniffer log, there is association-rsp sent from AP after received client’s association-req | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Connection\_4

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Connection\_4 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Validates that the client receive DHCP services in a timely manner | | |
| Pre-condition | 1) Wifi0/ wifi1 is binded with an open SSID  2) Client support wifi access through wifi0/ wifi1  3) Client and the SSID under test are configured as 802.11ng mode  4) Open debug for client monitor  ***\_deb capwap itk*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace table  3) Refresh SSID list on client  4) Try to associate the SSID under test  5) Ping mgt0 from client | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the DHCP process is successful  ***AH-81b680#sh log b | i itk***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  3) Ping mgt0 from client successfully  ***AH-81b680#sh l3 i***  ***Name IP Address Mode VLAN MAC State***  ***----------- --------------- -------- ------ -------------- -----***  ***Mgt0 10.155.30.93 - 1 0019:7781:b680 U***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.10 8 195M 78M -43(45) open none 00:08:26 1 Yes 0 11ng disabled 20MHz No data collecting...***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***C:\Users\cpliang>ipconfig***  ***Windows IP Configuration***  ***Wireless LAN adapter Wireless Network Connection:***  ***Connection-specific DNS Suffix . :***  ***Link-local IPv6 Address . . . . . : fe80::dc0c:5c47:3089:b0a5%13***  ***IPv4 Address. . . . . . . . . . . : 10.155.30.10***  ***Subnet Mask . . . . . . . . . . . : 255.255.255.0***  ***Default Gateway . . . . . . . . . : 10.155.30.254***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***C:\Users\cpliang>ping 10.155.30.93***  ***Pinging 10.155.30.93 with 32 bytes of data:***  ***Reply from 10.155.30.93: bytes=32 time=1ms TTL=64***  ***Reply from 10.155.30.93: bytes=32 time<1ms TTL=64***  ***Reply from 10.155.30.93: bytes=32 time<1ms TTL=64***  ***Reply from 10.155.30.93: bytes=32 time<1ms TTL=64***  ***Ping statistics for 10.155.30.93:***  ***Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),***  ***Approximate round trip times in milli-seconds:***  ***Minimum = 0ms, Maximum = 1ms, Average = 0ms*** | | |
| Test Result |  | | |

## ClientComp\_DellE5420\_11ng\_Auth

### ClientComp\_DellE5420\_11ng\_Auth\_1

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_1 | | |
| Priority | Accept | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Client get authentication with open mode | | |
| Pre-condition | 1) Config the SSID with open auth mode on client  2) Config the SSID with open auth mode on AP  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with open mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the open mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.10 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, Open auth is starting (at if=wifi0.1), level=1) step(1/2) SUCCESS***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 49dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 49dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-13 07:47:01 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 41dB), level=2) step(1/6) SUCCESS***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 192.168.100.2 8 117M 104M -39(54) open none 00:00:10 100 Yes 100 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 192.168.100.2***  ***PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.***  ***64 bytes from 192.168.100.2: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 192.168.100.2 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_2

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_2 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WEP/ WEP-104/ Open mode | | |
| Pre-condition | 1) Config the SSID with WEP/ Open auth mode on client  2) Config the SSID with WEP/ WEP-104/ Open auth mode on AP  ***ASCII Key, 1234567890123***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security protocol-suite wep-open 0 ascii-key \*\*\****  ***security-object zhxu default-user-profile-attr 100***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***interface mgt0.1 vlan 100***  ***interface mgt0.1 ip 192.168.100.1/24***  ***system led brightness off***  ***interface mgt0.1 dhcp-server ip-pool 192.168.100.2 192.168.100.10***  ***interface mgt0.1 dhcp-server enable***  ***config version 9***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***no bonjour-gateway enable***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-up-100 qos-policy def-user-qos vlan-id 100 attribute 100*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WEP/ WEP-104/ Open mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WEP/ WEP-104/ Open mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-16 07:21:36 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 07:21:36 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-16 07:21:36 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 07:21:36 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-16 07:21:36 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 07:21:36 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, Open auth is starting (at if=wifi0.1), level=1) step(1/2) SUCCESS***  ***……***  ***2012-07-16 07:21:36 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-16 07:21:36 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 54dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-16 07:21:36 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-16 07:21:36 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 55dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-16 07:21:36 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-16 07:21:36 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 53dB), level=2) step(1/6) SUCCESS***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 192.168.100.2 8 54M 54M -40(53) wep-open wep 00:20:24 100 Yes 100 11b/g static 20MHz No Good***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 192.168.100.2***  ***PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.***  ***64 bytes from 192.168.100.2: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 192.168.100.2 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_3

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_3 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WEP/ WEP-104/ Shared mode | | |
| Pre-condition | 1) Config the SSID with WEP/ Share auth mode on client  2) Store the shared passwd on client  3) Config the SSID with WEP/ WEP-104/ Shared auth mode on AP  ***ASCII Key, 1234567890123***  4) Capwap connection between AP and HM works well  5) Client and the SSID under test are configured as 802.11ng mode  6) Open debug for client monitor  ***\_deb capwap itk***  7) Config AP as the radius server  8) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security protocol-suite wep-shared 0 ascii-key \*\*\****  ***security-object zhxu default-user-profile-attr 100***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***interface mgt0.1 vlan 100***  ***interface mgt0.1 ip 192.168.100.1/24***  ***system led brightness off***  ***interface mgt0.1 dhcp-server ip-pool 192.168.100.2 192.168.100.10***  ***interface mgt0.1 dhcp-server enable***  ***config version 11***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***no bonjour-gateway enable***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-up-100 qos-policy def-user-qos vlan-id 100 attribute 100*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WEP/ WEP-104/ Shared mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WEP/ WEP-104/ Shared mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-16 07:47:45 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 07:47:45 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-16 07:47:45 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 07:47:45 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-16 07:47:45 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 07:47:45 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=42, Preshared auth is starting (at if=wifi0.1), level=1) step(1/2) SUCCESS***  ***……***  ***2012-07-16 07:47:45 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=1) step(0/0) SUCCESS***  ***……***  ***2012-07-16 07:47:45 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 50dB), level=1) step(0/0) SUCCESS***  ***……***  ***2012-07-16 07:47:45 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=47, Tx auth <shared> (frame 4, status 0, pwr 15dBm), level=1) step(0/0) SUCCESS***  ***……***  ***2012-07-16 07:47:45 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, Rx auth <shared> (frame 3, rssi 55dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-16 07:47:45 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=47, Tx auth <shared> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-16 07:47:45 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, Rx auth <shared> (frame 1, rssi 51dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-16 07:47:45 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-16 07:47:45 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 48dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 192.168.100.2 8 36M 48M -46(47) wep-shared wep 00:00:09 100 Yes 100 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 192.168.100.2***  ***PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.***  ***64 bytes from 192.168.100.2: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 192.168.100.2 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_4

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_4 | | |
| Priority | High | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WEP/ WEP-40/ Open mode | | |
| Pre-condition | 1) Config the SSID with WEP/ Open auth mode on client  2) Config the SSID with WEP/ WEP-40/ Open auth mode on AP  ***ASCII Key, 12345***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security protocol-suite wep-open 0 ascii-key \*\*\****  ***security-object zhxu default-user-profile-attr 100***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***interface mgt0.1 vlan 100***  ***interface mgt0.1 ip 192.168.100.1/24***  ***system led brightness off***  ***interface mgt0.1 dhcp-server ip-pool 192.168.100.2 192.168.100.10***  ***interface mgt0.1 dhcp-server enable***  ***config version 12***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***no bonjour-gateway enable***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-up-100 qos-policy def-user-qos vlan-id 100 attribute 100*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WEP/ WEP-40/ Open mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WEP/ WEP-40/ Open mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-16 08:03:00 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 08:03:00 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-16 08:03:00 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 08:03:00 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-16 08:03:00 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 08:03:00 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, Open auth is starting (at if=wifi0.1), level=1) step(1/2) SUCCESS***  ***……***  ***2012-07-16 08:03:00 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-16 08:03:00 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 55dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-16 08:03:00 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-16 08:03:00 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 54dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-16 08:03:00 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-16 08:03:00 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 48dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 192.168.100.2 8 24M 48M -40(53) wep-open wep 00:00:06 100 Yes 100 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 192.168.100.2***  ***PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.***  ***64 bytes from 192.168.100.2: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 192.168.100.2 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_5

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_5 | | |
| Priority | High | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WEP/ WEP-40/ Shared mode | | |
| Pre-condition | 1) Config the SSID with WEP/ Share auth mode on client  2) Store the shared passwd on client  3) Config the SSID with WEP/ WEP-40/ Shared auth mode on AP  ***ASCII Key, 12345***  4) Capwap connection between AP and HM works well  5) Client and the SSID under test are configured as 802.11ng mode  6) Open debug for client monitor  ***\_deb capwap itk***  7) Config AP as the radius server  8) Configuration on AP  ***AH-81b680# sh ru***  ***security-object zhxu***  ***security-object zhxu security protocol-suite wep-shared 0 ascii-key \*\*\****  ***security-object zhxu default-user-profile-attr 100***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***interface mgt0.1 vlan 100***  ***interface mgt0.1 ip 192.168.100.1/24***  ***system led brightness off***  ***interface mgt0.1 dhcp-server ip-pool 192.168.100.2 192.168.100.10***  ***interface mgt0.1 dhcp-server enable***  ***config version 13***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***no bonjour-gateway enable***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-up-100 qos-policy def-user-qos vlan-id 100 attribute 100*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WEP/ WEP-40/ Shared mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WEP/ WEP-40/ Shared mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-16 08:50:57 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 08:50:57 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-16 08:50:57 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-16 08:50:57 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, IP 192.168.100.2 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 08:50:57 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 08:50:57 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=42, Preshared auth is starting (at if=wifi0.1), level=1) step(1/2) SUCCESS***  ***……***  ***2012-07-16 08:50:57 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=1) step(0/0) SUCCESS***  ***……***  ***2012-07-16 08:50:57 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 48dB), level=1) step(0/0) SUCCESS***  ***……***  ***2012-07-16 08:50:57 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=47, Tx auth <shared> (frame 4, status 0, pwr 15dBm), level=1) step(0/0) SUCCESS***  ***……***  ***2012-07-16 08:50:57 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, Rx auth <shared> (frame 3, rssi 57dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-16 08:50:57 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=47, Tx auth <shared> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-16 08:50:57 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, Rx auth <shared> (frame 1, rssi 48dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-16 08:50:57 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-16 08:50:57 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 49dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 192.168.100.2 8 1M 1M -49(45) wep-shared wep 00:19:23 100 Yes 100 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 192.168.100.2***  ***PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.***  ***64 bytes from 192.168.100.2: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 192.168.100.2 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_6

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_6 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA2-PSK (WPA2 Personal)/ CCMP (AES) mode | | |
| Pre-condition | 1) Config the SSID with WPA2 Personal/ AES auth mode on client  2) Store the shared passwd on client  3) Config the SSID with WPA2-PSK (WPA2 Personal)/ CCMP (AES) auth mode on AP  ***ASCII Key, 12345678***  4) Capwap connection between AP and HM works well  5) Client and the SSID under test are configured as 802.11ng mode  6) Open debug for client monitor  ***\_deb capwap itk***  7) Config AP as the radius server  8) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security protocol-suite wpa2-aes-psk ascii-key \*\*\****  ***security-object zhxu default-user-profile-attr 100***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***interface mgt0.1 vlan 100***  ***interface mgt0.1 ip 192.168.100.1/24***  ***system led brightness off***  ***interface mgt0.1 dhcp-server ip-pool 192.168.100.2 192.168.100.10***  ***interface mgt0.1 dhcp-server enable***  ***config version 14***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***no bonjour-gateway enable***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-up-100 qos-policy def-user-qos vlan-id 100 attribute 100*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-PSK (WPA2 Personal)/ CCMP (AES) mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-PSK (WPA2 Personal)/ CCMP (AES) mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=40, WPA-PSK auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 55dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 55dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-16 09:13:21 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 48dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 192.168.100.2 8 130M 104M -40(51) wpa2-psk aes ccmp 00:00:58 100 Yes 100 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 192.168.100.2***  ***PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.***  ***64 bytes from 192.168.100.2: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 192.168.100.2 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_7

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_7 | | |
| Priority | High | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA2-PSK (WPA2 Personal)/ TKIP mode | | |
| Pre-condition | 1) Config the SSID with WPA2 Personal/ TKIP auth mode on client  2) Store the shared passwd on client  3) Config the SSID with WPA2-PSK (WPA2 Personal)/ TKIP auth mode on AP  ***ASCII Key, 12345678***  4) Capwap connection between AP and HM works well  5) Client and the SSID under test are configured as 802.11ng mode  6) Open debug for client monitor  ***\_deb capwap itk***  7) Config AP as the radius server  8) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security protocol-suite wpa2-tkip-psk ascii-key \*\*\****  ***security-object zhxu default-user-profile-attr 100***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***interface mgt0.1 vlan 100***  ***interface mgt0.1 ip 192.168.100.1/24***  ***system led brightness off***  ***report statistic period 1***  ***interface mgt0.1 dhcp-server ip-pool 192.168.100.2 192.168.100.10***  ***interface mgt0.1 dhcp-server enable***  ***config version 15***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***no bonjour-gateway enable***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-up-100 qos-policy def-user-qos vlan-id 100 attribute 100*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-PSK (WPA2 Personal)/ TKIP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-PSK (WPA2 Personal)/ TKIP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=40, WPA-PSK auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 50dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 47dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 50dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-16 09:30:21 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 49dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 192.168.100.2 8 18M 48M -39(49) wpa2-psk tkip 00:00:30 100 Yes 100 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 192.168.100.2***  ***PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.***  ***64 bytes from 192.168.100.2: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 192.168.100.2 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_8

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_8 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA-PSK (WPA Personal)/ CCMP (AES) mode | | |
| Pre-condition | 1) Config the SSID with WPA Personal/ AES auth mode on client  2) Store the shared passwd on client  3) Config the SSID with WPA-PSK (WPA Personal)/ CCMP (AES) auth mode on AP  ***ASCII Key, 12345678***  4) Capwap connection between AP and HM works well  5) Client and the SSID under test are configured as 802.11ng mode  6) Open debug for client monitor  ***\_deb capwap itk***  7) Config AP as the radius server  8) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security protocol-suite wpa-aes-psk ascii-key \*\*\****  ***security-object zhxu default-user-profile-attr 100***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***interface mgt0.1 vlan 100***  ***interface mgt0.1 ip 192.168.100.1/24***  ***system led brightness off***  ***interface mgt0.1 dhcp-server ip-pool 192.168.100.2 192.168.100.10***  ***interface mgt0.1 dhcp-server enable***  ***config version 16***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***no bonjour-gateway enable***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-up-100 qos-policy def-user-qos vlan-id 100 attribute 100*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA-PSK (WPA Personal)/ CCMP (AES) mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA-PSK (WPA Personal)/ CCMP (AES) mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, IP 192.168.100.2 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=40, WPA-PSK auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 54dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 55dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-17 02:19:34 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 49dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 192.168.100.2 8 117M 52M -39(54) wpa-psk aes ccmp 00:00:18 100 Yes 100 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 192.168.100.2***  ***PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.***  ***64 bytes from 192.168.100.2: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 192.168.100.2 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_9

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_9 | | |
| Priority | High | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA-PSK (WPA Personal)/ TKIP mode | | |
| Pre-condition | 1) Config the SSID with WPA Personal/ TKIP auth mode on client  2) Store the shared passwd on client  3) Config the SSID with WPA-PSK (WPA Personal)/ TKIP auth mode on AP  ***ASCII Key, 12345678***  4) Capwap connection between AP and HM works well  5) Client and the SSID under test are configured as 802.11ng mode  6) Open debug for client monitor  ***\_deb capwap itk***  7) Config AP as the radius server  8) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security protocol-suite wpa-tkip-psk ascii-key \*\*\****  ***security-object zhxu default-user-profile-attr 100***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***interface mgt0.1 vlan 100***  ***interface mgt0.1 ip 192.168.100.1/24***  ***system led brightness off***  ***interface mgt0.1 dhcp-server ip-pool 192.168.100.2 192.168.100.10***  ***interface mgt0.1 dhcp-server enable***  ***config version 17***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***no bonjour-gateway enable***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-up-100 qos-policy def-user-qos vlan-id 100 attribute 100*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA-PSK (WPA Personal)/ TKIP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA-PSK (WPA Personal)/ TKIP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-17 02:44:56 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 02:44:56 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-17 02:44:56 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 02:44:56 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-17 02:44:52 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 02:44:52 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-17 02:44:52 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-17 02:44:52 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-17 02:44:52 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-17 02:44:52 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-17 02:44:52 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=40, WPA-PSK auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-17 02:44:52 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-17 02:44:52 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 49dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-17 02:44:52 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-17 02:44:52 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 48dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-17 02:44:51 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-17 02:44:51 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 43dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 192.168.100.2 8 36M 54M -42(46) wpa-psk tkip 00:00:38 100 Yes 100 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 192.168.100.2***  ***PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.***  ***64 bytes from 192.168.100.2: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 192.168.100.2 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_10

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_10 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with Auto-(WPA or WPA2)-PSK/ Auto-TKIP or CCMP (AES) auth mode on AP | | |
| Pre-condition | 1) Config the SSID with WPA2 Personal/ AES auth mode on client  2) Store the shared passwd on client  3) Config the SSID with Auto-(WPA or WPA2)-PSK/ Auto-TKIP or CCMP (AES) auth mode on AP  ***ASCII Key, 12345678***  4) Capwap connection between AP and HM works well  5) Client and the SSID under test are configured as 802.11ng mode  6) Open debug for client monitor  ***\_deb capwap itk***  7) Config AP as the radius server  8) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security protocol-suite wpa-auto-psk ascii-key \*\*\****  ***security-object zhxu default-user-profile-attr 100***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***interface mgt0.1 vlan 100***  ***interface mgt0.1 ip 192.168.100.1/24***  ***system led brightness off***  ***interface mgt0.1 dhcp-server ip-pool 192.168.100.2 192.168.100.10***  ***interface mgt0.1 dhcp-server enable***  ***config version 18***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***no bonjour-gateway enable***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-up-100 qos-policy def-user-qos vlan-id 100 attribute 100*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-PSK (WPA2 Personal)/ CCMP (AES) mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-PSK (WPA2 Personal)/ CCMP (AES) mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, IP 192.168.100.2 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=40, WPA-PSK auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 47dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 45dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-17 02:57:48 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 46dB), level=2) step(1/6) SUCCESS***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 192.168.100.2 8 78M 52M -42(46) wpa2-psk aes ccmp 00:00:24 100 Yes 100 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 192.168.100.2***  ***PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.***  ***64 bytes from 192.168.100.2: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 192.168.100.2 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_11

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_11 | | |
| Priority | Accept | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ TLS mode | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ AES/ TLS auth mode on client  2) Config the SSID with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu100***  ***Certs= ca-cert: waterCA.pem, server-cert: gw1.crt, client-cert: czhong.p12***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa2-aes-8021x***  ***security-object zhxu default-user-profile-attr 100***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***interface mgt0.1 vlan 100***  ***interface mgt0.1 ip 192.168.100.1/24***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***interface mgt0.1 dhcp-server ip-pool 192.168.100.2 192.168.100.10***  ***interface mgt0.1 dhcp-server enable***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 28***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert waterCA.pem server-cert gw1.crt private-key gw1.key***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-100***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-up-100 qos-policy def-user-qos vlan-id 100 attribute 100*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ TLS mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ TLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-17 06:51:19 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 06:51:19 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-17 06:51:19 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, IP 192.168.100.2 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is SUCCESSfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-SUCCESS) identifier=8 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=147, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=20 length=210 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=65, RADIUS: accepted user 'zhxu100' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=20 length=151, User-Name=zhxu100 NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, received EAP packet (code=2 id=8 len=6) from STA: EAP Reponse-TLS (13), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=69, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=19 length=168, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/6) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=19 length=252, User-Name=zhxu100 NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=7 len=107) from STA: EAP Reponse-TLS (13), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=18 length=105, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=75, RADIUS: SSL negotiation, receive certificate and other message from client, level=2) step(4/6) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=220, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=18 length=1647, User-Name=zhxu100 NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=73, received EAP packet (code=2 id=6 len=1492) from STA: EAP Reponse-TLS (13), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=6 length=227, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=14 length=105, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=32, RADIUS: EAP start with type tls, level=2) step(1/6) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=14 length=151, User-Name=zhxu100 NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=13 length=105, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=13 length=139, User-Name=zhxu100 NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=97, received EAP packet (code=2 id=1 len=12) from STA: EAP Reponse-Identity (1), STA identity=zhxu100, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 51dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 48dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 50dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 192.168.100.2 8 1M 1M -40(51) wpa2-8021x aes ccmp 00:04:39 100 Yes 100 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 192.168.100.2***  ***PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.***  ***64 bytes from 192.168.100.2: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 192.168.100.2 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_12

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_12 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ PEAP mode | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ AES/ PEAP auth mode on client  ***User Credentials = Prompt automatically for username and password***  2) Config the SSID with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu100 / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa2-aes-8021x***  ***security-object zhxu default-user-profile-attr 100***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***interface mgt0.1 vlan 100***  ***interface mgt0.1 ip 192.168.100.1/24***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***interface mgt0.1 dhcp-server ip-pool 192.168.100.2 192.168.100.10***  ***interface mgt0.1 dhcp-server enable***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 29***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-100***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-up-100 qos-policy def-user-qos vlan-id 100 attribute 100*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ PEAP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ PEAP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-17 08:02:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 08:02:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-17 08:02:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, IP 192.168.100.2 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is SUCCESSfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-SUCCESS) identifier=9 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=147, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=29 length=210 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=65, RADIUS: accepted user 'zhxu100' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=29 length=225, User-Name=zhxu100 NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=9 len=80) from STA: EAP Reponse-PEAP (25), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=9 length=43, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=28 length=142, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: PEAP tunneled authentication was SUCCESSful, level=2) step(8/9) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=28 length=225, User-Name=zhxu100 NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=8 len=80) from STA: EAP Reponse-PEAP (25), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=43, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=27 length=142, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=38, RADIUS: PEAP inner tunneled conversion, level=2) step(7/9) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=27 length=225, User-Name=zhxu100 NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=7 len=80) from STA: EAP Reponse-PEAP (25), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=75, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=49, RADIUS: SSL negotiation is finished SUCCESSfully, level=2) step(6/9) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/9) SUCCESS***  ***……***  ***2012-07-17 08:02:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/9) SUCCESS***  ***……***  ***2012-07-17 08:02:06 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-17 08:02:06 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=21 length=139, User-Name=zhxu100 NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:02:06 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=97, received EAP packet (code=2 id=1 len=12) from STA: EAP Reponse-Identity (1), STA identity=zhxu100, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:01:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:01:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:01:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:01:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-17 08:01:58 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-17 08:01:58 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 52dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-17 08:01:58 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-17 08:01:58 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 50dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-17 08:01:58 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-17 08:01:58 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 50dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 192.168.100.2 8 130M 39M -39(52) wpa2-8021x aes ccmp 00:00:21 100 Yes 100 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 192.168.100.2***  ***PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.***  ***64 bytes from 192.168.100.2: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 192.168.100.2: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 192.168.100.2 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_13

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_13 | | |
| Priority | Middle | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ TTLS mode | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ AES/ TTLS auth mode on client  ***User Credentials = Prompt each time I connect***  2) Config the SSID with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa2-aes-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 37***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ TTLS mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ TTLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-18 06:45:49 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 06:45:49 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***2012-07-18 06:45:49 debug capwap: [capwap\_itk]: ITK: receive event(type=0, len=134) 138 bytes***  ***……***  ***2012-07-18 06:45:49 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is SUCCESSfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-SUCCESS) identifier=7 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=147, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=78 length=205 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=216, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=78 length=148, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, received EAP packet (code=2 id=7 len=6) from STA: EAP Reponse-TTLS (21), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=95, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=77 length=192, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: TTLS tunneled authentication was SUCCESSful, level=2) step(6/7) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=216, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=77 length=318, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=73, received EAP packet (code=2 id=6 len=176) from STA: EAP Reponse-TTLS (21), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=6 length=69, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/7) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/7) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/7) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type ttls, level=2) step(1/7) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 53dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 53dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 51dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -42(52) wpa2-8021x aes ccmp 00:05:08 1 Yes 1 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_14

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_14 | | |
| Priority | Middle | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ LEAP mode | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ AES/ LEAP auth mode on client  ***User Credentials = Prompt automatically for username and password***  2) Config the SSID with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa2-aes-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 37***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ LEAP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ LEAP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-18 08:14:15 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 08:14:15 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-18 08:14:15 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is SUCCESSfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, Sending EAP Packet to STA: code=2 (EAP-Response) identifier=3 length=36, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=148, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=106 length=180 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, RADIUS: Received challenge from the client, level=2) step(4/5) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=106 length=162, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=1 id=3 len=20) from STA: EAP Request-LEAP (17), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=3 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=105 length=101, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=47, RADIUS: MS-CHAP response verified successfully, level=2) step(3/5) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=48, RADIUS: Receive MS-CHAP response from the client, level=2) step(2/5) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=105 length=178, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=3 len=36) from STA: EAP Reponse-LEAP (17), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=3 length=20, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=104 length=117, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=59, RADIUS: Eap start with type leap and sent the AP challenge, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=104 length=148, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=103 length=103, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 46dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 46dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 46dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 175.5M 78M -45(48) wpa2-8021x aes ccmp 00:00:56 1 Yes 1 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_15

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_15 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA2-802.1X (WPA2 Enterprise)/ TKIP/ TLS mode | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ TKIP/ TLS auth mode on client  2) Config the SSID with WPA2-802.1X (WPA2 Enterprise)/ TKIP auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***Certs= ca-cert: waterCA.pem, server-cert: gw1.crt, client-cert: czhong.p12***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa2-tkip-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 38***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-802.1X (WPA2 Enterprise)/ TKIP/ TLS mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-802.1X (WPA2 Enterprise)/ TKIP/ TLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-18 10:36:07 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 10:36:07 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-18 10:36:07 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is SUCCESSfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-SUCCESS) identifier=8 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=85, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=117 length=168 , level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=64, RADIUS: accepted user 'czhong' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=117 length=150, User-Name=czhong NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, received EAP packet (code=2 id=8 len=6) from STA: EAP Reponse-TLS (13), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=69, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=116 length=127, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/6) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=116 length=251, User-Name=czhong NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=7 len=107) from STA: EAP Reponse-TLS (13), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=75, RADIUS: SSL negotiation, receive certificate and other message from client, level=2) step(4/6) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/6) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/6) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/6) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=32, RADIUS: EAP start with type tls, level=2) step(1/6) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=110 length=64, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=110 length=137, User-Name=czhong NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=96, received EAP packet (code=2 id=1 len=11) from STA: EAP Reponse-Identity (1), STA identity=czhong, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:05 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:04 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:04 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-18 10:36:04 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-18 10:36:04 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 51dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-18 10:36:04 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-18 10:36:04 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 49dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-18 10:36:04 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-18 10:36:04 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 49dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -45(48) wpa2-8021x tkip 00:01:29 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_16

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_16 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA2-802.1X (WPA2 Enterprise)/ TKIP/ PEAP mode | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ TKIP/ PEAP auth mode on client  ***User Credentials = Prompt automatically for username and password***  2) Config the SSID with WPA2-802.1X (WPA2 Enterprise)/ TKIP auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa2-tkip-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 38***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-802.1X (WPA2 Enterprise)/ TKIP/ PEAP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-802.1X (WPA2 Enterprise)/ TKIP/ PEAP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-18 08:47:16 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 08:47:16 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-18 08:47:16 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-18 08:47:14 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=74, ARP packets detected from/to station, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 08:47:14 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, IP 10.155.30.34 detected in ARP packets for station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is SUCCESSfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-SUCCESS) identifier=9 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=146, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=9 length=205 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=215, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=9 length=185, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=9 len=43) from STA: EAP Reponse-PEAP (25), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=9 length=43, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=86, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=8 length=140, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: PEAP tunneled authentication was SUCCESSful, level=2) step(8/9) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=215, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=8 length=185, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=8 len=43) from STA: EAP Reponse-PEAP (25), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=91, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=38, RADIUS: PEAP inner tunneled conversion, level=2) step(7/9) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=49, RADIUS: SSL negotiation is finished SUCCESSfully, level=2) step(6/9) SUCCESS***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK: receive event(type=0, len=127) 131 bytes***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/9) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/9) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/9) SUCCESS***  ***……***  ***2012-07-18 08:47:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-18 08:47:04 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:47:04 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:47:04 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-18 08:47:04 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 48dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-18 08:47:04 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-18 08:47:03 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 48dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-18 08:47:03 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-18 08:47:03 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 48dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -45(48) wpa2-8021x tkip 00:01:29 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_17

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_17 | | |
| Priority | Middle | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA2-802.1X (WPA2 Enterprise)/ TKIP/ TTLS mode | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ TKIP/ TTLS auth mode on client  ***User Credentials = Prompt each time I connect***  2) Config the SSID with WPA2-802.1X (WPA2 Enterprise)/ TKIP auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa2-tkip-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 38***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-802.1X (WPA2 Enterprise)/ TKIP/ TTLS mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-802.1X (WPA2 Enterprise)/ TKIP/ TTLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-18 09:21:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 09:21:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-18 09:21:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is SUCCESSfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-SUCCESS) identifier=7 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=148, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=127 length=205 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=127 length=148, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, received EAP packet (code=2 id=7 len=6) from STA: EAP Reponse-TTLS (21), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=95, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=126 length=192, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: TTLS tunneled authentication was SUCCESSful, level=2) step(6/7) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/7) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/7) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/7) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type ttls, level=2) step(1/7) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=121 length=103, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-18 09:21:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:20:59 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:20:59 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:20:59 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:20:59 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-18 09:20:59 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 55dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-18 09:20:59 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-18 09:20:59 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 54dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-18 09:20:58 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-18 09:20:58 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 51dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -45(48) wpa2-8021x tkip 00:01:29 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_18

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_18 | | |
| Priority | Middle | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA2-802.1X (WPA2 Enterprise)/ TKIP/ LEAP mode | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ TKIP/ LEAP auth mode on client  ***User Credentials = Prompt automatically for username and password***  2) Config the SSID with WPA2-802.1X (WPA2 Enterprise)/ TKIP auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa2-tkip-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 38***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-802.1X (WPA2 Enterprise)/ TKIP/ LEAP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-802.1X (WPA2 Enterprise)/ TKIP/ LEAP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-18 09:33:42 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 09:33:42 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-18 09:33:42 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is SUCCESSfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, Sending EAP Packet to STA: code=2 (EAP-Response) identifier=3 length=36, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=148, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=169 length=180 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, RADIUS: Received challenge from the client, level=2) step(4/5) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=169 length=162, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=1 id=3 len=20) from STA: EAP Request-LEAP (17), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-SUCCESS) identifier=3 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=168 length=101, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=47, RADIUS: MS-CHAP response verified SUCCESSfully, level=2) step(3/5) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=48, RADIUS: Receive MS-CHAP response from the client, level=2) step(2/5) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=168 length=178, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=3 len=36) from STA: EAP Reponse-LEAP (17), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=3 length=20, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=59, RADIUS: Eap start with type leap and sent the AP challenge, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=166 length=103, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-18 09:33:38 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:30 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:30 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:29 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-18 09:33:29 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-18 09:33:29 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 56dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-18 09:33:29 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-18 09:33:29 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 56dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-18 09:33:29 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-18 09:33:29 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 50dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -45(48) wpa2-8021x tkip 00:01:29 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_19

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_19 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA-802.1X (WPA Enterprise)/ CCMP (AES)/ TLS mode | | |
| Pre-condition | 1) Config the SSID with WPA Enterprise/ AES/ TLS auth mode on client  2) Config the SSID with WPA-802.1X (WPA Enterprise)/ CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***Certs= ca-cert: waterCA.pem, server-cert: gw1.crt, client-cert: czhong.p12***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa-aes-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 40***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert waterCA.pem server-cert gw1.crt private-key gw1.key***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA-802.1X (WPA Enterprise)/ CCMP (AES)/ TLS mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA-802.1X (WPA Enterprise)/ CCMP (AES)/ TLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 02:05:14 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:05:14 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 02:05:14 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=8 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=84, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=53 length=168 , level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=64, RADIUS: accepted user 'czhong' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=218, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=53 length=150, User-Name=czhong NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, received EAP packet (code=2 id=8 len=6) from STA: EAP Reponse-TLS (13), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=69, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=52 length=127, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=218, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=52 length=251, User-Name=czhong NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=7 len=107) from STA: EAP Reponse-TLS (13), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=75, RADIUS: SSL negotiation, receive certificate and other message from client, level=2) step(4/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=32, RADIUS: EAP start with type tls, level=2) step(1/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=86, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=46 length=64, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 54dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 54dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 52dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -44(45) wpa-8021x aes ccmp 00:03:20 1 Yes 1 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_20

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_20 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA-802.1X (WPA Enterprise)/ CCMP (AES)/ PEAP mode | | |
| Pre-condition | 1) Config the SSID with WPA Enterprise/ AES/ PEAP auth mode on client  ***User Credentials = Prompt automatically for username and password***  2) Config the SSID with WPA-802.1X (WPA Enterprise)/ CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa-aes-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 42***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA-802.1X (WPA Enterprise)/ CCMP (AES)/ PEAP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA-802.1X (WPA Enterprise)/ CCMP (AES)/ PEAP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 02:40:35 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:40:35 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 02:40:35 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 02:40:35 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=74, ARP packets detected from/to station, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:40:35 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, IP 10.155.30.34 detected in ARP packets for station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=9 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=146, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=9 length=205 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=215, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=9 length=185, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=9 len=43) from STA: EAP Reponse-PEAP (25), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=9 length=43, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=86, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=8 length=140, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: PEAP tunneled authentication was successful, level=2) step(8/9) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=215, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=8 length=185, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=8 len=43) from STA: EAP Reponse-PEAP (25), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=91, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=38, RADIUS: PEAP inner tunneled conversion, level=2) step(7/9) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=38, RADIUS: PEAP inner tunneled conversion, level=2) step(7/9) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=49, RADIUS: SSL negotiation is finished successfully, level=2) step(6/9) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/9) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/9) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/9) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 02:40:32 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:40:26 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:40:26 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:40:26 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:40:26 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 02:40:26 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 55dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 02:40:26 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 02:40:26 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 55dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 02:40:26 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 02:40:26 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 53dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -43(51) wpa-8021x aes ccmp 00:01:20 1 Yes 1 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_21

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_21 | | |
| Priority | Middle | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA-802.1X (WPA Enterprise)/ CCMP (AES)/ TTLS mode | | |
| Pre-condition | 1) Config the SSID with WPA Enterprise/ AES/ TTLS auth mode on client  ***User Credentials = Prompt each time I connect***  2) Config the SSID with WPA-802.1X (WPA Enterprise)/ CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa-aes-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 42***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA-802.1X (WPA Enterprise)/ CCMP (AES)/ TTLS mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA-802.1X (WPA Enterprise)/ CCMP (AES)/ TTLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 02:57:10 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:57:10 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 02:57:10 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=7 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=147, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=66 length=205 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=216, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=66 length=148, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, received EAP packet (code=2 id=7 len=6) from STA: EAP Reponse-TTLS (21), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=95, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=65 length=192, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: TTLS tunneled authentication was successful, level=2) step(6/7) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=216, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=65 length=318, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=73, received EAP packet (code=2 id=6 len=176) from STA: EAP Reponse-TTLS (21), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=6 length=69, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/7) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/7) SUCCESS***  ***……***  ***2012-07-19 02:57:07 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/7) SUCCESS***  ***……***  ***2012-07-19 02:57:06 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type ttls, level=2) step(1/7) SUCCESS***  ***……***  ***2012-07-19 02:57:06 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:57:06 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:57:06 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=60 length=103, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:57:06 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 02:57:06 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:56:59 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:56:59 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:56:59 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:56:59 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 02:56:59 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 51dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 02:56:59 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 02:56:59 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 52dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 02:56:59 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 02:56:59 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 53dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -43(51) wpa-8021x aes ccmp 00:01:20 1 Yes 1 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_22

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_22 | | |
| Priority | Middle | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA-802.1X (WPA Enterprise)/ CCMP (AES)/ LEAP mode | | |
| Pre-condition | 1) Config the SSID with WPA Enterprise/ AES/ LEAP auth mode on client  ***User Credentials = Prompt automatically for username and password***  2) Config the SSID with WPA-802.1X (WPA Enterprise)/ CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa-aes-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 42***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA-802.1X (WPA Enterprise)/ CCMP (AES)/ LEAP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA-802.1X (WPA Enterprise)/ CCMP (AES)/ LEAP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 03:08:56 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 03:08:56 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 03:08:56 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, Sending EAP Packet to STA: code=2 (EAP-Response) identifier=3 length=36, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=148, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=101 length=180 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, RADIUS: Received challenge from the client, level=2) step(4/5) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=101 length=162, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=1 id=3 len=20) from STA: EAP Request-LEAP (17), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=3 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=100 length=101, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=47, RADIUS: MS-CHAP response verified successfully, level=2) step(3/5) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=48, RADIUS: Receive MS-CHAP response from the client, level=2) step(2/5) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=100 length=178, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=3 len=36) from STA: EAP Reponse-LEAP (17), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=3 length=20, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=59, RADIUS: Eap start with type leap and sent the AP challenge, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 03:08:54 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:08:47 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:08:47 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:08:47 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:08:47 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 03:08:47 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 54dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 03:08:47 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 03:08:47 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 50dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 03:08:47 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 03:08:47 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 53dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -43(51) wpa-8021x aes ccmp 00:01:20 1 Yes 1 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_23

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_23 | | |
| Priority | Accept | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA-802.1X (WPA Enterprise)/ TKIP/ TLS mode | | |
| Pre-condition | 1) Config the SSID with WPA Enterprise/ TKIP/ TLS auth mode on client  2) Config the SSID with WPA-802.1X (WPA Enterprise)/ TKIP auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***Certs= ca-cert: waterCA.pem, server-cert: gw1.crt, client-cert: czhong.p12***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa-tkip-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 41***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert waterCA.pem server-cert gw1.crt private-key gw1.key***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA-802.1X (WPA Enterprise)/ TKIP/ TLS mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA-802.1X (WPA Enterprise)/ TKIP/ TLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 02:23:37 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:23:37 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 02:23:37 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:23:37 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=8 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=83, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=8 length=168 , level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=64, RADIUS: accepted user 'czhong' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=8 length=150, User-Name=czhong NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, received EAP packet (code=2 id=8 len=6) from STA: EAP Reponse-TLS (13), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=69, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=86, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=7 length=127, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/6) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=7 length=251, User-Name=czhong NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=7 len=107) from STA: EAP Reponse-TLS (13), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=75, RADIUS: SSL negotiation, receive certificate and other message from client, level=2) step(4/6) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/6) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/6) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/6) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=32, RADIUS: EAP start with type tls, level=2) step(1/6) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=85, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=1 length=64, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=96, received EAP packet (code=2 id=1 len=11) from STA: EAP Reponse-Identity (1), STA identity=czhong, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 52dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 54dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 02:23:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 50dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 54M 48M -44(50) wpa-8021x tkip 00:01:11 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_24

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_24 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA-802.1X (WPA Enterprise)/ TKIP/ PEAP mode | | |
| Pre-condition | 1) Config the SSID with WPA Enterprise/ TKIP/ PEAP auth mode on client  ***User Credentials = Prompt automatically for username and password***  2) Config the SSID with WPA-802.1X (WPA Enterprise)/ TKIP auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa-tkip-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 43***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA-802.1X (WPA Enterprise)/ TKIP/ PEAP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA-802.1X (WPA Enterprise)/ TKIP/ PEAP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 03:28:30 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 03:28:30 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 03:28:30 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 03:28:30 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 03:28:26 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 03:28:26 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=9 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=146, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=9 length=205 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=215, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=9 length=185, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=9 len=43) from STA: EAP Reponse-PEAP (25), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=9 length=43, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=86, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=8 length=140, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: PEAP tunneled authentication was successful, level=2) step(8/9) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=215, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=8 length=185, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=8 len=43) from STA: EAP Reponse-PEAP (25), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=91, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=38, RADIUS: PEAP inner tunneled conversion, level=2) step(7/9) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=38, RADIUS: PEAP inner tunneled conversion, level=2) step(7/9) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=49, RADIUS: SSL negotiation is finished successfully, level=2) step(6/9) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/9) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/9) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/9) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 03:28:25 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:28:18 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:28:18 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:28:17 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:28:17 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 03:28:17 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 51dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 03:28:17 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 03:28:17 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 52dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 03:28:17 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 03:28:17 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 49dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 54M 48M -40(53) wpa-8021x tkip 00:01:12 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_25

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_25 | | |
| Priority | Middle | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA-802.1X (WPA Enterprise)/ TKIP/ TTLS mode | | |
| Pre-condition | 1) Config the SSID with WPA Enterprise/ TKIP/ TTLS auth mode on client  ***User Credentials = Prompt each time I connect***  2) Config the SSID with WPA-802.1X (WPA Enterprise)/ TKIP auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa-tkip-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 43***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA-802.1X (WPA Enterprise)/ TKIP/ TTLS mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA-802.1X (WPA Enterprise)/ TKIP/ TTLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 03:39:06 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 03:39:06 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 03:39:06 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=7 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=147, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=48 length=205 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=216, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=48 length=148, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, received EAP packet (code=2 id=7 len=6) from STA: EAP Reponse-TTLS (21), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=95, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=47 length=192, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: TTLS tunneled authentication was successful, level=2) step(6/7) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=216, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=47 length=318, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=73, received EAP packet (code=2 id=6 len=176) from STA: EAP Reponse-TTLS (21), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=6 length=69, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/7) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/7) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/7) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type ttls, level=2) step(1/7) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=42 length=103, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 03:39:02 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:38:56 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:38:56 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:38:56 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-19 03:38:56 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 03:38:56 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 53dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 03:38:56 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 03:38:56 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 52dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 03:38:56 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 03:38:56 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 47dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 54M 48M -40(53) wpa-8021x tkip 00:01:12 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_26

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_26 | | |
| Priority | Middle | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WPA-802.1X (WPA Enterprise)/ TKIP/ LEAP mode | | |
| Pre-condition | 1) Config the SSID with WPA Enterprise/ TKIP/ LEAP auth mode on client  ***User Credentials = Prompt automatically for username and password***  2) Config the SSID with WPA-802.1X (WPA Enterprise)/ TKIP auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa-tkip-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 43***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA-802.1X (WPA Enterprise)/ TKIP/ LEAP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA-802.1X (WPA Enterprise)/ TKIP/ LEAP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 05:48:24 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 05:48:24 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 05:48:24 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, Sending EAP Packet to STA: code=2 (EAP-Response) identifier=3 length=36, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=148, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=212 length=180 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, RADIUS: Received challenge from the client, level=2) step(4/5) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=212 length=162, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=1 id=3 len=20) from STA: EAP Request-LEAP (17), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=3 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=211 length=101, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=47, RADIUS: MS-CHAP response verified successfully, level=2) step(3/5) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=48, RADIUS: Receive MS-CHAP response from the client, level=2) step(2/5) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=211 length=178, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=3 len=36) from STA: EAP Reponse-LEAP (17), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=3 length=20, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=59, RADIUS: Eap start with type leap and sent the AP challenge, level=2) step(1/5) SUCCESS***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK: receive event(type=0, len=137) 141 bytes***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=209 length=103, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 05:48:20 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-19 05:48:14 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 05:48:14 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 54dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 05:48:14 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 05:48:14 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 57dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 05:48:14 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 05:48:14 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 53dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 54M 48M -40(53) wpa-8021x tkip 00:01:12 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_27

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_27 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with Auto-(WPA or WPA2)-EAP (802.1X) / Auto-TKIP or CCMP (AES) / TLS mode | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ AES/ TLS auth mode on client  2) Config the SSID with Auto-(WPA or WPA2)-EAP (802.1X) / Auto-TKIP or CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu100***  ***Certs= ca-cert: waterCA.pem, server-cert: gw1.crt, client-cert: czhong.p12***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa-auto-8021x***  ***security-object zhxu default-user-profile-attr 100***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***interface mgt0.1 vlan 100***  ***interface mgt0.1 ip 192.168.100.1/24***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***interface mgt0.1 dhcp-server ip-pool 192.168.100.2 192.168.100.10***  ***interface mgt0.1 dhcp-server enable***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 28***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert waterCA.pem server-cert gw1.crt private-key gw1.key***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-100***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-up-100 qos-policy def-user-qos vlan-id 100 attribute 100*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ TLS mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ TLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-17 06:51:19 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 06:51:19 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-17 06:51:19 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, IP 192.168.100.2 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is SUCCESSfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-SUCCESS) identifier=8 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=147, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=20 length=210 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=65, RADIUS: accepted user 'zhxu100' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=20 length=151, User-Name=zhxu100 NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, received EAP packet (code=2 id=8 len=6) from STA: EAP Reponse-TLS (13), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=69, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=19 length=168, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/6) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=19 length=252, User-Name=zhxu100 NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=7 len=107) from STA: EAP Reponse-TLS (13), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=18 length=105, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=75, RADIUS: SSL negotiation, receive certificate and other message from client, level=2) step(4/6) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=220, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=18 length=1647, User-Name=zhxu100 NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=73, received EAP packet (code=2 id=6 len=1492) from STA: EAP Reponse-TLS (13), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=6 length=227, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=14 length=105, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=32, RADIUS: EAP start with type tls, level=2) step(1/6) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=14 length=151, User-Name=zhxu100 NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=13 length=105, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=13 length=139, User-Name=zhxu100 NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=97, received EAP packet (code=2 id=1 len=12) from STA: EAP Reponse-Identity (1), STA identity=zhxu100, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 51dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 48dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-17 06:51:07 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 50dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 192.168.100.2 8 1M 1M -40(51) wpa2-8021x aes ccmp 00:04:39 100 Yes 100 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_28

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_28 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with Auto-(WPA or WPA2)-EAP (802.1X) / Auto-TKIP or CCMP (AES) / PEAP mode | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ AES/ PEAP auth mode on client  ***User Credentials = Prompt automatically for username and password***  2) Config the SSID with Auto-(WPA or WPA2)-EAP (802.1X) / Auto-TKIP or CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa-auto-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 34***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ PEAP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ PEAP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-18 03:21:17 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 03:21:17 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***2012-07-18 03:21:17 debug capwap: [capwap\_itk]: ITK: receive event(type=0, len=134) 138 bytes***  ***……***  ***2012-07-18 03:21:17 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is SUCCESSfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-SUCCESS) identifier=9 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=148, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=141 length=205 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=141 length=222, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=9 len=80) from STA: EAP Reponse-PEAP (25), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=9 length=43, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=140 length=140, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: PEAP tunneled authentication was SUCCESSful, level=2) step(8/9) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=140 length=222, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=8 len=80) from STA: EAP Reponse-PEAP (25), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=43, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=38, RADIUS: PEAP inner tunneled conversion, level=2) step(7/9) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=49, RADIUS: SSL negotiation is finished SUCCESSfully, level=2) step(6/9) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/9) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/9) SUCCESS***  ***……***  ***2012-07-18 03:21:13 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-18 03:21:06 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 03:21:06 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-18 03:21:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-18 03:21:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 49dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-18 03:21:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-18 03:21:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 50dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-18 03:21:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-18 03:21:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 47dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 195M 117M -40(49) wpa2-8021x aes ccmp 02:31:43 1 Yes 1 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_29

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_29 | | |
| Priority | Middle | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Client get authentication with Auto-(WPA or WPA2)-EAP (802.1X) / Auto-TKIP or CCMP (AES) / TTLS mode | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ AES/ TTLS auth mode on client  ***User Credentials = Prompt each time I connect***  2) Config the SSID with Auto-(WPA or WPA2)-EAP (802.1X) / Auto-TKIP or CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa-auto-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 36***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ TTLS mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ TTLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-18 06:45:49 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 06:45:49 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***2012-07-18 06:45:49 debug capwap: [capwap\_itk]: ITK: receive event(type=0, len=134) 138 bytes***  ***……***  ***2012-07-18 06:45:49 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is SUCCESSfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-SUCCESS) identifier=7 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=147, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=78 length=205 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=216, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=78 length=148, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, received EAP packet (code=2 id=7 len=6) from STA: EAP Reponse-TTLS (21), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=95, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=77 length=192, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: TTLS tunneled authentication was SUCCESSful, level=2) step(6/7) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=216, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=77 length=318, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=73, received EAP packet (code=2 id=6 len=176) from STA: EAP Reponse-TTLS (21), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=6 length=69, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/7) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/7) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/7) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type ttls, level=2) step(1/7) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:46 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 53dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 53dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-18 06:45:39 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 51dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -42(52) wpa2-8021x aes ccmp 00:05:08 1 Yes 1 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_30

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_30 | | |
| Priority | Middle | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with Auto-(WPA or WPA2)-EAP (802.1X) / Auto-TKIP or CCMP (AES) / LEAP mode | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ AES/ LEAP auth mode on client  ***User Credentials = Prompt automatically for username and password***  2) Config the SSID with Auto-(WPA or WPA2)-EAP (802.1X) / Auto-TKIP or CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa-auto-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 36***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ LEAP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ LEAP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-18 08:14:15 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 08:14:15 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-18 08:14:15 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is SUCCESSfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, Sending EAP Packet to STA: code=2 (EAP-Response) identifier=3 length=36, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=148, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=106 length=180 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, RADIUS: Received challenge from the client, level=2) step(4/5) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=106 length=162, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=1 id=3 len=20) from STA: EAP Request-LEAP (17), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=3 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=105 length=101, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=47, RADIUS: MS-CHAP response verified successfully, level=2) step(3/5) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=48, RADIUS: Receive MS-CHAP response from the client, level=2) step(2/5) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=105 length=178, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=3 len=36) from STA: EAP Reponse-LEAP (17), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=3 length=20, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=104 length=117, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=59, RADIUS: Eap start with type leap and sent the AP challenge, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=104 length=148, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=103 length=103, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:12 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 46dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 46dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-18 08:14:06 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 46dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 175.5M 78M -45(48) wpa2-8021x aes ccmp 00:00:56 1 Yes 1 11ng disabled 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_31

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_31 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WEP-802.1X/ WEP-104/ TLS mode | | |
| Pre-condition | 1) Config the SSID with WEP-802.1X/ WEP-104/ TLS auth mode on client  2) Config the SSID with WEP-802.1X/ WEP-104 auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu***  ***Certs= ca-cert: waterCA.pem, server-cert: gw1.crt, client-cert: czhong.p12***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wep104-8021x rekey-period 600***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 3***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert waterCA.pem server-cert gw1.crt private-key gw1.key***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WEP-802.1X/ WEP-104/ TLS mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WEP-802.1X/ WEP-104/ TLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=40, sending DWEP unicast key (at if=wifi0.1), level=1) step(4/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=42, sending DWEP broadcast key (at if=wifi0.1), level=1) step(3/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=8 length=4, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=85, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=174 length=168 , level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=64, RADIUS: accepted user 'czhong' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=174 length=150, User-Name=czhong NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, received EAP packet (code=2 id=8 len=6) from STA: EAP Reponse-TLS (13), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=69, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=173 length=127, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=173 length=251, User-Name=czhong NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=7 len=107) from STA: EAP Reponse-TLS (13), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=6, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=75, RADIUS: SSL negotiation, receive certificate and other message from client, level=2) step(4/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=32, RADIUS: EAP start with type tls, level=2) step(1/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=167 length=64, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=96, received EAP packet (code=2 id=1 len=11) from STA: EAP Reponse-Identity (1), STA identity=czhong, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 48dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 50dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 47dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -48(45) wep-8021x wep 00:02:18 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_32

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_32 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WEP-802.1X/ WEP-104/ PEAP mode | | |
| Pre-condition | 1) Config the SSID with WEP-802.1X/ WEP-104/ PEAP auth mode on client  ***User Credentials = Prompt automatically for username and password***  2) Config the SSID with WEP-802.1X/ WEP-104 auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wep104-8021x rekey-period 600***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 44***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WEP-802.1X/ WEP-104/ PEAP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WEP-802.1X/ WEP-104/ PEAP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=40, sending DWEP unicast key (at if=wifi0.1), level=1) step(4/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=42, sending DWEP broadcast key (at if=wifi0.1), level=1) step(3/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=9 length=4, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=146, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=9 length=205 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=215, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=9 length=185, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=9 len=43) from STA: EAP Reponse-PEAP (25), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=9 length=43, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=86, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=8 length=140, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: PEAP tunneled authentication was successful, level=2) step(8/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=215, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=8 length=185, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=8 len=43) from STA: EAP Reponse-PEAP (25), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=91, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=38, RADIUS: PEAP inner tunneled conversion, level=2) step(7/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=38, RADIUS: PEAP inner tunneled conversion, level=2) step(7/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=49, RADIUS: SSL negotiation is finished successfully, level=2) step(6/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/5) SUCCESS***  ***……***  ***capwap\_itk]: ITK: Send capwap-event(type=4, cookie=327272, len=65)***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 47dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 53dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 46dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -48(45) wep-8021x wep 00:02:18 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_33

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_33 | | |
| Priority | Middle | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WEP-802.1X/ WEP-104/ TTLS mode | | |
| Pre-condition | 1) Config the SSID with WEP-802.1X/ WEP-104/ TTLS auth mode on client  ***User Credentials = Prompt each time I connect***  2) Config the SSID with WEP-802.1X/ WEP-104 auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wep104-8021x rekey-period 600***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 44***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WEP-802.1X/ WEP-104/ TTLS mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WEP-802.1X/ WEP-104/ TTLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=40, sending DWEP unicast key (at if=wifi0.1), level=1) step(4/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=42, sending DWEP broadcast key (at if=wifi0.1), level=1) step(3/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=7 length=4, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=147, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=84 length=205 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=216, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=84 length=148, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, received EAP packet (code=2 id=7 len=6) from STA: EAP Reponse-TTLS (21), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=95, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=83 length=192, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: TTLS tunneled authentication was successful, level=2) step(6/7) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/7) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/7) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/7) SUCCESS***  ***……***  ***2012-07-19 06:36:14 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type ttls, level=2) step(1/7) SUCCESS***  ***……***  ***2012-07-19 06:36:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=78 length=103, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:14 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 06:36:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 55dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 55dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 50dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -48(45) wep-8021x wep 00:02:18 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_34

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_34 | | |
| Priority | Middle | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WEP-802.1X/ WEP-104/ LEAP mode | | |
| Pre-condition | 1) Config the SSID with WEP-802.1X/ WEP-104/ LEAP auth mode on client  ***User Credentials = Prompt automatically for username and password***  2) Config the SSID with WEP-802.1X/ WEP-104 auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wep104-8021x rekey-period 600***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 44***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WEP-802.1X/ WEP-104/ LEAP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WEP-802.1X/ WEP-104/ LEAP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=40, sending DWEP unicast key (at if=wifi0.1), level=1) step(4/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=42, sending DWEP broadcast key (at if=wifi0.1), level=1) step(3/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, Sending EAP Packet to STA: code=2 (EAP-Response) identifier=3 length=36, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=148, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=141 length=180 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, RADIUS: Received challenge from the client, level=2) step(4/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=141 length=162, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=1 id=3 len=20) from STA: EAP Request-LEAP (17), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=3 length=4, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=140 length=101, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=47, RADIUS: MS-CHAP response verified successfully, level=2) step(3/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=48, RADIUS: Receive MS-CHAP response from the client, level=2) step(2/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=140 length=178, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=3 len=36) from STA: EAP Reponse-LEAP (17), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=3 length=20, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=59, RADIUS: Eap start with type leap and sent the AP challenge, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=138 length=103, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 53dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 58dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 55dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -48(45) wep-8021x wep 00:02:18 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_35

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_35 | | |
| Priority | High | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WEP-802.1X/ WEP-40/ TLS mode | | |
| Pre-condition | 1) Config the SSID with WEP-802.1X/ WEP-40/ TLS auth mode on client  2) Config the SSID with WEP-802.1X/ WEP-40 auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu***  ***Certs= ca-cert: waterCA.pem, server-cert: gw1.crt, client-cert: czhong.p12***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wep40-8021x rekey-period 600***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 4***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert waterCA.pem server-cert gw1.crt private-key gw1.key***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WEP-802.1X/ WEP-40/ TLS mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WEP-802.1X/ WEP-40/ TLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=40, sending DWEP unicast key (at if=wifi0.1), level=1) step(4/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=42, sending DWEP broadcast key (at if=wifi0.1), level=1) step(3/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=8 length=4, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=85, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=174 length=168 , level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=64, RADIUS: accepted user 'czhong' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=174 length=150, User-Name=czhong NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, received EAP packet (code=2 id=8 len=6) from STA: EAP Reponse-TLS (13), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=69, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=173 length=127, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=219, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=173 length=251, User-Name=czhong NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=7 len=107) from STA: EAP Reponse-TLS (13), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=6, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=75, RADIUS: SSL negotiation, receive certificate and other message from client, level=2) step(4/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=32, RADIUS: EAP start with type tls, level=2) step(1/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=167 length=64, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=96, received EAP packet (code=2 id=1 len=11) from STA: EAP Reponse-Identity (1), STA identity=czhong, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/5) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 48dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 50dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 07:06:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 47dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -48(45) wep-8021x wep 00:02:18 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_36

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_36 | | |
| Priority | High | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WEP-802.1X/ WEP-40/ PEAP mode | | |
| Pre-condition | 1) Config the SSID with WEP-802.1X/ WEP-40/ PEAP auth mode on client  ***User Credentials = Prompt automatically for username and password***  2) Config the SSID with WEP-802.1X/ WEP-40 auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wep40-8021x rekey-period 600***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 5***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WEP-802.1X/ WEP-40/ PEAP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WEP-802.1X/ WEP-40/ PEAP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=40, sending DWEP unicast key (at if=wifi0.1), level=1) step(4/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=42, sending DWEP broadcast key (at if=wifi0.1), level=1) step(3/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=9 length=4, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=146, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=9 length=205 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=215, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=9 length=185, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=9 len=43) from STA: EAP Reponse-PEAP (25), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=9 length=43, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=86, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=8 length=140, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: PEAP tunneled authentication was successful, level=2) step(8/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=215, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=8 length=185, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=8 len=43) from STA: EAP Reponse-PEAP (25), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=91, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=38, RADIUS: PEAP inner tunneled conversion, level=2) step(7/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=38, RADIUS: PEAP inner tunneled conversion, level=2) step(7/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=49, RADIUS: SSL negotiation is finished successfully, level=2) step(6/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 06:13:39 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/5) SUCCESS***  ***……***  ***capwap\_itk]: ITK: Send capwap-event(type=4, cookie=327272, len=65)***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 47dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 53dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 06:13:33 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 46dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -48(45) wep-8021x wep 00:02:18 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_37

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_37 | | |
| Priority | Middle | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WEP-802.1X/ WEP-40/ TTLS mode | | |
| Pre-condition | 1) Config the SSID with WEP-802.1X/ WEP-40/ TTLS auth mode on client  ***User Credentials = Prompt each time I connect***  2) Config the SSID with WEP-802.1X/ WEP-40 auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wep40-8021x rekey-period 600***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 5***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WEP-802.1X/ WEP-40/ TTLS mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WEP-802.1X/ WEP-40/ TTLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=40, sending DWEP unicast key (at if=wifi0.1), level=1) step(4/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=42, sending DWEP broadcast key (at if=wifi0.1), level=1) step(3/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=7 length=4, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=147, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=84 length=205 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=216, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=84 length=148, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, received EAP packet (code=2 id=7 len=6) from STA: EAP Reponse-TTLS (21), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=95, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=83 length=192, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: TTLS tunneled authentication was successful, level=2) step(6/7) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/7) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/7) SUCCESS***  ***……***  ***2012-07-19 06:36:15 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/7) SUCCESS***  ***……***  ***2012-07-19 06:36:14 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type ttls, level=2) step(1/7) SUCCESS***  ***……***  ***2012-07-19 06:36:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=78 length=103, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:14 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 06:36:14 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 55dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 55dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 06:36:09 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 50dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -48(45) wep-8021x wep 00:02:18 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_38

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_38 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication with WEP-802.1X/ WEP-40/ LEAP mode | | |
| Pre-condition | 1) Config the SSID with WEP-802.1X/ WEP-40/ LEAP auth mode on client  ***User Credentials = Prompt automatically for username and password***  2) Config the SSID with WEP-802.1X/ WEP-40 auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***user = zhxu / 12345678***  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client monitor  ***\_deb capwap itk***  6) Config AP as the radius server  7) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wep40-8021x rekey-period 600***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 5***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WEP-802.1X/ WEP-40/ LEAP mode  5) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WEP-802.1X/ WEP-40/ LEAP mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=40, sending DWEP unicast key (at if=wifi0.1), level=1) step(4/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=42, sending DWEP broadcast key (at if=wifi0.1), level=1) step(3/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=71, Sending EAP Packet to STA: code=2 (EAP-Response) identifier=3 length=36, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=148, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=141 length=180 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, RADIUS: Received challenge from the client, level=2) step(4/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=141 length=162, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=1 id=3 len=20) from STA: EAP Request-LEAP (17), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=3 length=4, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=140 length=101, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=47, RADIUS: MS-CHAP response verified successfully, level=2) step(3/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=48, RADIUS: Receive MS-CHAP response from the client, level=2) step(2/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=217, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=140 length=178, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=3 len=36) from STA: EAP Reponse-LEAP (17), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=3 length=20, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=59, RADIUS: Eap start with type leap and sent the AP challenge, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=88, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=138 length=103, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 06:53:49 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5, level=2) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/5) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 53dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 58dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 06:53:42 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 55dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -48(45) wep-8021x wep 00:02:18 1 Yes 1 11b/g static 20MHz No data collecting...***  7) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_Auth\_39

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Auth\_39 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Topo1 | | |
| Description | Client get authentication via CWP process | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ AES/ TLS auth mode on client  2) Config the SSID with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  ***Certs= ca-cert: waterCA.pem, server-cert: gw1.crt, client-cert: czhong.p12***  3) Config “Enable a captive web portal with use policy acceptance”  4) Capwap connection between AP and HM works well  5) Client and the SSID under test are configured as 802.11ng mode  6) Open debug for client monitor  ***\_deb capwap itk***  7) Config AP as the radius server  8) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa2-aes-8021x***  ***security-object zhxu security additional-auth-method captive-web-portal reg-user-profile-attr 1***  ***security-object zhxu default-user-profile-attr 1***  ***security-object zhxu web-server web-page mandatory-field 0 optional-field 0***  ***security-object zhxu web-server index-file eula.html***  ***security-object zhxu web-directory zhxu-cwp***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 6***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert waterCA.pem server-cert gw1.crt private-key gw1.key***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the process of client get authentication with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ TLS mode  5) Visit a http address via IE browser on client  ***http://www.bing.com***  6) Send uplink traffic from client for 5 minutes | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Check the probe-req/ probe-rsp process is correct and regular  3) Check the auth-req/ auth-rsp process is correct and regular  4) Check the assoc-req/ assoc-rsp process is correct and regular  5) Check the WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES)/ TLS mode auth is successful  6) Check the DHCP process is successful  ***AH-81b680#sh lo b | i itk***  ***……***  ***2012-07-19 02:05:14 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:05:14 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-19 02:05:14 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=8 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=84, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=53 length=168 , level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=64, RADIUS: accepted user 'czhong' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=218, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=53 length=150, User-Name=czhong NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, received EAP packet (code=2 id=8 len=6) from STA: EAP Reponse-TLS (13), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=69, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=52 length=127, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=218, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=52 length=251, User-Name=czhong NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-90:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=7 len=107) from STA: EAP Reponse-TLS (13), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=75, RADIUS: SSL negotiation, receive certificate and other message from client, level=2) step(4/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=32, RADIUS: EAP start with type tls, level=2) step(1/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, received EAP packet (code=2 id=2 len=6) from STA: EAP Reponse-Nak (3), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=6, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=86, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=46 length=64, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 54dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 54dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-19 02:05:11 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b690) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 52dB), level=2) step(1/6) SUCCESS***  ***……***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -44(45) wpa-8021x aes ccmp 00:03:20 1 Yes 1 11ng disabled 20MHz No data collecting...***  7) Check the process of CWP  ***When try to visit http://***[***www.bing.com***](http://www.bing.com)***, the page redirect to http://1.1.1.1/reg.php***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh lo b | i cwp***  ***……***  ***2012-07-19 09:08:58 info ah\_auth: Guest CWP user is registered on if wifi0.1***  ***2012-07-19 09:08:58 notice ah\_auth: A CWP user registered from interface wifi0.1: MAC=0024:d7f4:26a8, IP=1.1.1.102***  ***……***  8) Check there is no reconnection of client during sending traffic  ***AH-81b680#ping 10.155.30.34***  ***PING 10.155.30.34 (10.155.30.34) 56(84) bytes of data.***  ***64 bytes from 10.155.30.34: icmp\_seq=1 ttl=64 time=0.217 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=2 ttl=64 time=0.157 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=3 ttl=64 time=0.164 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=4 ttl=64 time=0.156 ms***  ***64 bytes from 10.155.30.34: icmp\_seq=5 ttl=64 time=0.162 ms***  ***--- 10.155.30.34 ping statistics ---***  ***5 packets transmitted, 5 received, 0% packet loss, time 3999ms***  ***rtt min/avg/max/mdev = 0.156/0.171/0.217/0.024 ms*** | | |
| Test Result |  | | |

## ClientComp\_DellE5420\_11ng\_OsDetect

### ClientComp\_DellE5420\_11ng\_OsDetect\_1

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_OsDetect\_1 | | |
| Priority | Accept | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Support of OS detection for client | | |
| Pre-condition | 1) Config the SSID with open auth mode on client  2) Config the SSID with open auth mode on AP  3) Capwap connection between AP and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Open debug for client  ***\_deb capwap itk***  ***\_deb auth dhcp\_fp***  6) Config AP as the radius server | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get the client associated with the SSID under test  4) Check the OS of client detected by AP | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Client get association successfully  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 192.168.85.10 11 195M 1M -46(48) open none 00:01:07 1 Yes 0 11ng disabled 20MHz No data collecting...***  3) Check client’s OS detected by AP  ***AH-81b680#sh lo b | i os***  ***2012-07-25 02:19:33 info ah\_auth: detect station(0024:d7f4:26a8) hostname(cpliang-PC) os(Windows 7/Vista) via DHCP fingerprint***  ***2012-07-25 02:19:33 debug ah\_auth: [auth\_dhcp\_fp]: doesn't need to update station(0024:d7f4:26a8) os(Windows 7/Vista) to AUTH***  ***2012-07-25 02:19:33 debug ah\_auth: [auth\_dhcp\_fp]: mapped OS: Windows 7/Vista***  ***2012-07-25 02:19:33 debug ah\_auth: [auth\_dhcp\_fp]: no maping os found in user configure database***  ***2012-07-25 02:19:33 debug ah\_auth: [auth\_dhcp\_fp]: mapping station(0024:d7f4:26a8) to os...***  ***2012-07-25 02:19:31 info ah\_auth: auth send os info(Windows 7/Vista) trap for 0024:d7f4:26a8 to Capwap successfully***  ***2012-07-25 02:19:30 notice ah\_auth: ah\_rt\_sta\_update\_hostname: 0024:d7f4:26a8(hostname=cpliang-PC)***  ***2012-07-25 02:19:30 info ah\_auth: detect station(0024:d7f4:26a8) hostname(cpliang-PC) os(Windows 7/Vista) via DHCP fingerprint***  ***2012-07-25 02:19:30 debug ah\_auth: [auth\_dhcp\_fp]: doesn't need to update station(0024:d7f4:26a8) os(Windows 7/Vista) to AUTH***  ***2012-07-25 02:19:30 debug ah\_auth: [auth\_dhcp\_fp]: mapped OS: Windows 7/Vista***  ***2012-07-25 02:19:30 debug ah\_auth: [auth\_dhcp\_fp]: no maping os found in user configure database***  ***2012-07-25 02:19:30 debug ah\_auth: [auth\_dhcp\_fp]: mapping station(0024:d7f4:26a8) to os...*** | | |
| Test Result |  | | |

## ClientComp\_DellE5420\_11ng\_WMM

### ClientComp\_DellE5420\_11ng\_WMM\_1

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_WMM\_1 | | |
| Priority | Accept | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Support of VoIP service with UL traffic from client | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ AES/ PEAP auth mode on client\_01 under test  2) Config the SSID with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on AP  3) Config SIP settings on client  ***Install X-lite on client***  4) Config SIP server which is used to connect with client  ***Install Brekeke SIP server***  5) Capwap connection between AP and HM works well  6) Client and the SSID under test are configured as 802.11ng mode  7) Open ALG and debug taps for SIP  ***alg sip enable***  ***\_ff dst-port 5060***  ***\_kdeb fe basic***  ***\_kdeb fe detail***  8) Config AP as the radius server  9) Config the SSID on another client\_02 with WPA2 Enterprise/ AES/ PEAP auth mode  10) Configuration on AP  ***zhxu-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa2-aes-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***hostname zhxu-81b680***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 15***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1***  ***alg sip enable*** | | |
| Test procedure | 1) Get the client\_01 under test associated with the SSID under test  2) Get another client\_02 associated with the SSID under test  3) Run VoIP traffic from client\_01 to client\_02 for 5 mins  4) Check the msg interaction during VoIP service | | |
| Expect result | 1) Client\_01 and Client\_02 get association successfully  ***Client\_01, under test, 0024:d7f4:26a8, 10.155.30.34***  ***Client\_02, Not under test, 2477:0312:d9c0, 10.155.30.100***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***zhxu-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 195M 78M -37(57) wpa2-8021x aes ccmp 02:10:31 1 Yes 1 11ng disabled 20MHz No Good***  ***Ifname=wifi1.1, Ifindex=16, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***2477:0312:d9c0 10.155.30.100 153 195M 195M -44(50) wpa2-8021x aes ccmp 02:05:51 1 Yes 1 11na disabled 20MHz No Good***  3) Run VoIP traffic from client\_01 to client\_02 successfully  ***zhxu-81b680#sh alg sip ca***  ***Total number of SIP calls : 2***  ***(user=N/A, MAC=d067:e544:c77d) <-> (user=, MAC=2477:0312:d9c0)***  ***From:"10.155.30.80"<sip:8888@10.155.30.80>***  ***To:"9999"<sip:9999@10.155.30.80>***  ***Call-id:4a6dbf347c03a956MTVhYTkxMTZlNjJkNzBlM2U1ZWNlZDYxMjhlYjA4ZmM.***  ***Media :audio 10.155.30.34:58119 <-> 10.155.30.100:10887***  ***Media :audio 10.155.30.34:58118 <-> 10.155.30.100:10886***  ***(user=zhxu, MAC=0024:d7f4:26a8) <-> (user=N/A, MAC=d067:e544:c77d)***  ***From:"10.155.30.80"<sip:8888@10.155.30.80>***  ***To:"9999"<sip:9999@10.155.30.80>***  ***Call-id:4a6dbf347c03a956MTVhYTkxMTZlNjJkNzBlM2U1ZWNlZDYxMjhlYjA4ZmM.***  ***Media :audio 10.155.30.34:58119 <-> 10.155.30.100:10887***  ***Media :audio 10.155.30.34:58118 <-> 10.155.30.100:10886***  4) Check the msg interaction during VoIP service  ***zhxu-81b680#sh lo b | i fe***  ***……***  ***2012-07-24 04:34:07 debug kernel: [fe]: QoS: ingress pkt fwd(wifi1.1) profile=1 qos=6***  ***2012-07-24 04:34:07 debug kernel: [fe]: update from-access counters 1115 bytes***  ***2012-07-24 04:34:07 debug kernel: [fe]: refreshed IP session, id [2] ageout 600 sec, alg sip flags 0x24480***  ***2012-07-24 04:34:07 debug kernel: [fe]: IP session id [2] found***  ***2012-07-24 04:34:07 debug kernel: [fe]: fflow acl 0x0/0x0, rflow acl 0x0/0x0***  ***2012-07-24 04:34:07 debug kernel: [fe]: fflow 2477:0312:d9c0->d067:e544:c77d flag 0x65000, rflow d067:e544:c77d->2477:0312:d9c0 flag 0xe1210***  ***……***  ***2012-07-24 04:33:58 debug kernel: [fe]: QoS: pkt forwarded (eth0) qos=6 profile=1***  ***2012-07-24 04:33:58 debug kernel: [fe]: eth0 Tx 0024:d7f4:26a8 -> d067:e544:c77d type 0x0800 976 bytes***  ***2012-07-24 04:33:58 debug kernel: [fe]: send ALG control pkt 986 bytes to app, payload length 934 bytes***  ***2012-07-24 04:33:58 debug kernel: [fe]: QoS: ingress pkt fwd(wifi0.1) profile=1 qos=6***  ***2012-07-24 04:33:58 debug kernel: [fe]: update from-access counters 976 bytes***  ***2012-07-24 04:33:58 debug kernel: [fe]: refreshed IP session, id [1] ageout 600 sec, alg sip flags 0x24480***  ***2012-07-24 04:33:58 debug kernel: [fe]: IP session id [1] found***  ***2012-07-24 04:33:58 debug kernel: [fe]: fflow acl 0x0/0x0, rflow acl 0x0/0x0***  ***2012-07-24 04:33:58 debug kernel: [fe]: fflow 0024:d7f4:26a8->d067:e544:c77d flag 0x65000, rflow d067:e544:c77d->0024:d7f4:26a8 flag 0xe1210***  ***2012-07-24 04:33:58 debug kernel: [fe]: MAC session (id [57]) found*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_WMM\_2

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_WMM\_2 | | |
| Priority | Middle | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Support of VoIP service with DL traffic to client | | |
| Pre-condition |  | | |
| Test procedure |  | | |
| Expect result |  | | |
| Test Result |  | | |

## ClientComp\_DellE5420\_11ng\_PS

### ClientComp\_DellE5420\_11ng\_PS\_1

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_PS\_1 | | |
| Priority | Accept | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Support of U-APSD PS mode | | |
| Pre-condition | 1) Enable U-APSD power save mode on AP  2) Enable U-APSD power save mode on client and specify the WMM AC  3) Turn on UAPSD and power debug on AP  ***\_kdebug wifi-driver wifi0/1 extend uapsd***  ***\_kdebug wifi-driver wifi0.x/1.x power***  4) Run wireless sniffer which is tuned in the same channel as the wifi interface under test | | |
| Test procedure | 1) Get the client associated with the SSID unter test  2) Keep the client silent for a moment  3) After 5 mins, generate the corresponding AC with U-APSD traffic from the server to the client via AP  4) Check WMM U-APSD frames in the sniffer trace | | |
| Expect result | 1) Client get association successfully  2) Client should set the U-APSD enable flag in the corresponding AC in the QoS capability and WMM capability of Association request  3) AP set the U-APSD enable in the QoS field of the WMM capability in the Beacon, prob response and association response  4) After client is silent for a while, client sends out a null data or other packets to the AP and set power save mode in the Frame Control field  5) Client should send trigger frame to the AP to retrieve the data; and the trigger frame usually is null data frame, but could be any type of frames, like control frames. | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_PS\_2

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_PS\_2 | | |
| Priority | Accept | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Support of PS-Poll PS mode | | |
| Pre-condition | 1) Enable PS-Poll power save mode on AP  2) Enable PS-Poll power save mode on client  3) Turn on power debug on AP  ***\_kdebug wifi-driver wifi0.x/1.x power***  ***\_kdebug wifi-driver wifi0/1 extend uapsd***  4) Run wireless sniffer which is tuned in the same channel as the wifi interface under test  5) Configuration on AP  ***AH-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface mgt0 hive Aerohive***  ***interface wifi0 ssid zhxu***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 10***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***no bonjour-gateway enable***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Get the client associated with the SSID unter test  2) Keep the client silent for a moment  3) After 5 mins, generate traffic from the server to the client via AP  4) Check PS-Poll frames in the sniffer trace | | |
| Expect result | 1) The PS mode of the SSID under test is U-APSD disabled  ***AH-81b680#sh ssid zhxu | i "uapsd state"***  ***UAPSD state: Disabled***  2) Client get association successfully  ***AH-81b680#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 195M 78M -40(54) open none 00:00:33 1 Yes 1 11ng disabled 20MHz No data collecting...***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***AH-81b680#sh lo b | i pow***  ***2012-07-20 02:47:45 debug kernel: wifi0.1: ieee80211\_parse\_htcap:SM powersave disabled***  3) Client should set U-APSD disabled in Association request  3) AP set the PS-Poll enable in Beacon, prob response and association response  4) After client is silent for a while, client sends the frame which indicates that the client goes to power save mode    5) Client sends PS-Poll packet to the AP to retrieve the data  6) AP sends the buffered data to the client after received the PS-Poll from the client  7) Client should send another PS-Poll to the AP to retrieve another data frame | | |
| Test Result | *Fail to let client enter ps mode* | | |

## ClientComp\_DellE5420\_11ng\_Roaming

### ClientComp\_DellE5420\_11ng\_ Roaming\_1

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Roaming\_1 | | |
| Priority | Accept | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Support of L2 Fast Roaming (Pre-auth) | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ AES/ PEAP auth mode on client  2) Config the SSID with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on both AP1 and AP2  3) Capwap connection between APs and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Run wireless sniffer which is tuned in the same channel as the wifi interface under test  6) Open debug for client monitor  ***\_deb capwap itk***  7) Config AP1 as the radius server  8) Configuration on AP  ***zhxu-81b680#sh ru***  ***security-object zhxu***  ***security-object zhxu security aaa radius-server primary 10.155.30.93***  ***security-object zhxu security aaa radius-server accounting primary 10.155.30.93***  ***security-object zhxu security protocol-suite wpa2-aes-8021x***  ***security-object zhxu default-user-profile-attr 1***  ***ssid zhxu***  ***ssid zhxu security-object zhxu***  ***hive Aerohive***  ***hive Aerohive password \*\*\****  ***interface wifi0 radio channel 8***  ***interface wifi0 radio power 20***  ***interface wifi1 mode access***  ***interface wifi1 radio channel 48***  ***interface wifi1 radio power 20***  ***interface mgt0 hive Aerohive***  ***interface wifi1 ssid zhxu***  ***system led brightness off***  ***hostname zhxu-81b680***  ***interface mgt0 ip 10.155.30.93 255.255.255.0***  ***no interface mgt0 dhcp client***  ***ip route net 0.0.0.0 0.0.0.0 gateway 10.155.30.254***  ***config version 14***  ***config rollback enable***  ***snmp location zhxu@floor01***  ***aaa radius-server local sta-auth ca-cert Default\_CA.pem server-cert Default-Server\_cert.pem private-key Default-Server\_key.pem***  ***aaa radius-server local db-type local***  ***aaa radius-server local enable***  ***no bonjour-gateway enable***  ***aaa radius-server local user-group zhxu-UserGroup-1***  ***capwap client server name 10.155.31.201***  ***capwap client dtls hm-defined-passphrase \*\*\* key-id 1***  ***capwap client vhm-name home***  ***no capwap client dtls negotiation enable***  ***data-collection enable***  ***user-profile zhxu-UserProfile-vlan1 qos-policy def-user-qos vlan-id 1 attribute 1*** | | |
| Test procedure | 1) Add the client to monitor  ***exec client-monitor 0024:d7f4:26a8***  2) Check if the client exist in the trace Table  3) Get client associated with the SSID on AP1 unter test  ***show station***  ***show route***  4) Send uplink traffic from client for 5 minutes  5) On AP1 and AP2, check the PMK in roaming cach  ***show roaming cache***  6) Force the client roam from AP1 to AP2  ***On AP1,***  ***no in w0 ssid zhxu***  ***no in w1 ssid zhxu***  ***On AP2,***  ***show station***  ***show route***  7) Check re-auth behavior on radius server  8) Check roaming frames in the sniffer trace | | |
| Expect result | 1) Client is in the trace table once added into the list  ***AH-81b680#\_sh client-monitor***  ***Kernel:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  ***Application:***  ***Client Trace Table(sta\_num=1):***  ***Entry(0024:d7f4:26a8 cookie\_num=2): 327272 1***  ***Dhcp Probe Array(num=0):***  2) Client get association with AP1 successfully  ***zhxu-81b680# sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 1M 1M -37(51) wpa2-8021x aes ccmp 00:19:28 1 Yes 1 11ng disabled 20MHz No data collecting...***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***zhxu-81b680#sh route***  ***Route table:***  ***flag: (S)tatic, (I)nterface (L)ocal (T)unnel (O)wn***  ***sta nhop oif metric upid flag***  ***---------------------------------------------------------***  ***0000:0000:0000 0019:7781:b680 eth0 0 0 L O***  ***0019:7781:b694 0019:7781:b680 wifi0.1 0 4096 IL***  ***0019:7781:b682 0019:7781:b680 red0 0 4096 IL***  ***0019:7781:b683 0019:7781:b680 agg0 0 4096 IL***  ***0019:7781:b680 0019:7781:b680 eth0 0 4096 IL***  ***0019:7781:b681 0019:7781:b680 eth1 0 4096 IL***  ***0024:d7f4:26a8 0019:7781:b680 wifi0.1 0 1 L O***  ***0019:7781:b6a8 0019:7781:b680 wifi1.1 0 4096 IL***  3) Make sure the local cache and roaming cache has the same PMK on AP1 and AP2  ***zhxu-81b680#sh roa c***  ***Roaming Cache Table:***  ***UID=User profile group ID; PMK=Pairwise Master Key;***  ***TLC=PMK Time Left in Cache; Life=PMK Life; A=authenticated; L=CWP Logged In; D=Disconnected; M=managed by MDM***  ***Roaming for this AP: enabled***  ***Maximum Caching Time: 3600 seconds***  ***Caching update interval: 60 seconds***  ***Caching update times: 60***  ***Roaming hops: 1***  ***Broadcast way: access backhaul***  ***No. Supplicant Authenticator Size UID PMK PMKID Life Age TLC Hop ALDM***  ***--- -------------- -------------- ---- --- ----- ----- -------- -------- -------- --- ----***  ***0 0024:d7f4:26a8 4018:b14e:3654 512 1 d946\* b3e1\* 1800 1511 3590 1 YNNN***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***zhxu-4e3640#sh roa c***  ***Roaming Cache Table:***  ***UID=User profile group ID; PMK=Pairwise Master Key;***  ***TLC=PMK Time Left in Cache; Life=PMK Life; A=authenticated; L=CWP Logged In; D=Disconnected; M=managed by MDM***  ***Roaming for this AP: enabled***  ***Maximum Caching Time: 3600 seconds***  ***Caching update interval: 60 seconds***  ***Caching update times: 60***  ***Roaming hops: 1***  ***Broadcast way: access backhaul***  ***No. Supplicant Authenticator Size UID PMK PMKID Life Age TLC Hop ALDM***  ***--- -------------- -------------- ---- --- ----- ----- -------- -------- -------- --- ----***  ***0 0024:d7f4:26a8 4018:b14e:3654 512 1 d946\* b3e1\* 1800 1518 3583 0 YNNN***  4) After roaming, client connect to AP2 successfully  ***zhxu-4e3640#sh st***  ***Chan=channel number; Pow=Power in dBm;***  ***A-Mode=Authentication mode; Cipher=Encryption mode;***  ***A-Time=Associated time; Auth=Authenticated;***  ***UPID=User profile Identifier; Phymode=Physical mode;***  ***Ifname=wifi0.1, Ifindex=14, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  ***0024:d7f4:26a8 10.155.30.34 8 156M 156M -42(47) wpa2-8021x aes ccmp 02:28:37 1 Yes 1 11ng disabled 20MHz No data collecting...***  ***Ifname=wifi1.1, Ifindex=16, SSID=zhxu:***  ***Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release Station-State***  ***-------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***zhxu-4e3640#***  ***zhxu-4e3640#sh route***  ***Route table:***  ***flag: (S)tatic, (I)nterface (L)ocal (T)unnel (O)wn***  ***sta nhop oif metric upid flag***  ***---------------------------------------------------------***  ***0000:0000:0000 4018:b14e:3640 eth0 0 0 L O***  ***4018:b14e:3668 4018:b14e:3640 wifi1.1 0 4096 IL***  ***4018:b14e:3640 4018:b14e:3640 eth0 0 4096 IL***  ***4018:b14e:3641 4018:b14e:3640 eth1 0 4096 IL***  ***4018:b14e:3642 4018:b14e:3640 red0 0 4096 IL***  ***4018:b14e:3643 4018:b14e:3640 agg0 0 4096 IL***  ***4018:b14e:3654 4018:b14e:3640 wifi0.1 0 4096 IL***  ***0024:d7f4:26a8 4018:b14e:3640 wifi0.1 0 1 L O***  ***Total route entries: 8***  5) Check the roaming process and make sure no re-auth when roaming happened  ***On AP1,***  ***zhxu-81b680#sh lo b | i itk***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=52, Tx deauth (reason 2 <prior-auth-invalid>, pwr 15dBm), level=1) step(0/0) FAILED***  ***……***  ***2012-07-23 04:18:01 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=34, DHCP session completed for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-23 04:18:01 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=56, DHCP server sent out DHCP ACKNOWLEDGE message to station, level=1) step(4/4) SUCCESS***  ***……***  ***2012-07-23 04:18:01 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=37, station sent out DHCP REQUEST message, level=1) step(3/4) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=3 (EAP-Success) identifier=9 length=4, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=45, PMK is got from RADIUS server (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=147, Receive message from RADIUS Server: code=2 (Access-Accept) identifier=23 length=205 RADIUS\_ATTR\_TUNNEL\_TYPE=10 RADIUS\_ATTR\_TUNNEL\_MIDDLE\_TYPE=1 RA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=62, RADIUS: accepted user 'zhxu' through the NAS at 10.155.30.93., level=2) step(0/0) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=216, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=23 length=187, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-94:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=9 len=43) from STA: EAP Reponse-PEAP (25), level=2) step(1/8) SUCCESS***  ***……***  ***apwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=9 length=43, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=22 length=140, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=51, RADIUS: PEAP tunneled authentication was successful, level=2) step(8/9) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=216, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=22 length=187, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-94:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=8 len=43) from STA: EAP Reponse-PEAP (25), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=91, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=87, Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=21 length=188, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=38, RADIUS: PEAP inner tunneled conversion, level=2) step(7/9) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=216, Send message to RADIUS Server(10.155.30.93): code=1 (Access-Request) identifier=21 length=235, User-Name=zhxu NAS-IP-Address=10.155.30.93 Called-Station-Id=00-19-77-81-B6-94:zhxu Calling-Station-Id=00-24-D7-F4-26-A8, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=72, received EAP packet (code=2 id=7 len=91) from STA: EAP Reponse-PEAP (25), level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=70, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=59, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=49, RADIUS: SSL negotiation is finished successfully, level=2) step(6/9) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=35, RADIUS: SSL connection established, level=2) step(5/9) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=67, RADIUS: SSL negotiation, send server certificate and other message, level=2) step(3/9) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=54, RADIUS: SSL negotiation, receive client hello message, level=2) step(2/9) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(RADIUS) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=33, RADIUS: EAP start with type peap, level=2) step(1/9) SUCCESS***  ***……***  ***2012-07-23 04:17:58 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=93, received EAP packet (code=2 id=1 len=9) from STA: EAP Reponse-Identity (1), STA identity=zhxu, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:51 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:51 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=29, received EAPOL-Start from STA, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:51 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=69, Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5, level=2) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:51 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:17:51 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-23 04:17:51 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 52dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-23 04:17:51 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-23 04:17:51 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 51dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-23 04:17:51 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-23 04:17:51 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(0019:7781:b694) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 51dB), level=2) step(1/6) SUCCESS***  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  *- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -*  ***zhxu-81b680#sh lo b | i de-auth***  ***2012-07-23 04:18:12 notice ah\_auth: Station 0024:d7f4:26a8 is de-authenticated from 0019:7781:b694 thru SSID zhxu***  ***On AP2,***  ***zhxu-4e3640#sh lo b | i itk***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(DHCP) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=36, IP 10.155.30.34 assigned for station, level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=55, Authentication is successfully finished (at if=wifi0.1), level=0) step(0/0) SUCCESS***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=26, PTK is set (at if=wifi0.1), level=1) step(7/8) SUCCESS***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=51, Received 4/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(6/8) SUCCESS***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=50, Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(5/8) SUCCESS***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=51, Received 2/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(4/8) SUCCESS***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=50, Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1), level=1) step(3/8) SUCCESS***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=43, PMK is got from local cache (at if=wifi0.1), level=1) step(2/8) SUCCESS***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(AUTH) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=43, IEEE802.1X auth is starting (at if=wifi0.1), level=1) step(1/8) SUCCESS***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=44, Tx assoc resp <accept> (status 0, pwr 15dBm), level=0) step(6/6) SUCCESS***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=24, Rx assoc req (rssi 48dB), level=0) step(5/6) SUCCESS***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=45, Tx auth <open> (frame 2, status 0, pwr 15dBm), level=0) step(4/6) SUCCESS***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=35, Rx auth <open> (frame 1, rssi 46dB), level=0) step(3/6) SUCCESS***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=25, Tx probe resp (pwr 15dBm), level=0) step(2/6) SUCCESS***  ***……***  ***2012-07-23 04:18:12 debug capwap: [capwap\_itk]: ITK-ct: module(802.11) in AP(4018:b14e:3654) report sta(0024:d7f4:26a8): claim(len=34, Rx <unicast> probe req (rssi 49dB), level=2) step(1/6) SUCCESS***  ***……***  6) Check the roaming msg captured by sniffer  ***On AP1, There is process for PMK derivation (eap process)***    ***On AP2, there is no process for PMK*** | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_ Roaming\_2

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Roaming\_2 | | |
| Priority | Accept | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Support of L2 Fast Roaming (OKC) | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ AES/ PEAP auth mode on client  2) Config the SSID with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on both AP1 and AP2  3) Capwap connection between APs and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Run wireless sniffer which is tuned in the same channel as the wifi interface under test  6) Open debug for client  ***debug auth basic***  7) Config AP as the radius server | | |
| Test procedure | 1) Get client associated with the SSID on AP1 unter test  ***show auth***  ***show ssid xxx station***  ***show route***  2) Send uplink traffic from client for 5 minutes  3) On AP1 and AP2, check the PMK in roaming cach  ***show roaming cache***  4) Force the client roam from AP1 to AP2  ***show auth***  ***show ssid xxx station***  ***show route***  5) Check re-auth behavior on radius server  6) Check roaming frames in the sniffer trace | | |
| Expect result | 1) Client get association with AP1 successfully  2) Make sure the local cache and roaming cache has the same PMK on AP1 and AP2  3) After roaming, client connect to AP2 successfully  4) Make sure no re-auth on radius server when roaming happened  5) The roaming time should be less than 1 second | | |
| Test Result |  | | |

### ClientComp\_DellE5420\_11ng\_ Roaming\_3

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_Roaming\_3 | | |
| Priority | Accept | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Support of L2 Fast Roaming (802.11r) | | |
| Pre-condition | 1) Config the SSID with WPA2 Enterprise/ AES/ PEAP auth mode on client  2) Config the SSID with WPA2-802.1X (WPA2 Enterprise)/ CCMP (AES) auth mode, and the Authentication mode on Radius as TLS/ PEAP/ TTLS/ LEAP supported on both AP1 and AP2  3) Capwap connection between APs and HM works well  4) Client and the SSID under test are configured as 802.11ng mode  5) Run wireless sniffer which is tuned in the same channel as the wifi interface under test  6) Open debug for client  ***debug auth basic***  7) Config AP as the radius server | | |
| Test procedure | 1) Get client associated with the SSID on AP1 unter test  ***show auth***  ***show ssid xxx station***  ***show route***  2) Send uplink traffic from client for 5 minutes  3) On AP1 and AP2, check the PMK in roaming cach  ***show roaming cache***  4) Force the client roam from AP1 to AP2  ***show auth***  ***show ssid xxx station***  ***show route***  5) Check re-auth behavior on radius server  6) Check roaming frames in the sniffer trace | | |
| Expect result | 1) Client get association with AP1 successfully  2) Make sure the local cache and roaming cache has the same PMK on AP1 and AP2  3) After roaming, client connect to AP2 successfully  4) Make sure no re-auth on radius server when roaming happened  5) The roaming time should be less than 1 second | | |
| Test Result |  | | |

## ClientComp\_DellE5420\_11ng\_802.11w

### ClientComp\_DellE5420\_11ng\_802.11w\_1

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | ClientComp\_DellE5420\_11ng\_802.11w\_1 | | |
| Priority | Middle | Automation Flag | Yes |
| Topology to use | Topo1 | | |
| Description | Support of 802.11w | | |
| Pre-condition |  | | |
| Test procedure |  | | |
| Expect result | 1) Management frames have been encrypted | | |
| Test Result |  | | |