Use this Cheat Sheet for Common Wireless Issues

Contents

Introduction

This document describes a cheat sheet that parses through debugs (usually, debug client <mac address>) for common wireless issues.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on all AireOS controllers.

- Controllers- 440x, the 5508, 5520, 75xx, 85xx, 2504, 3504, and vWLC, as well as WISMs.
- Although many concepts are identical in Converged Access IOS® XE controllers and switches, this document does not apply to them as outputs and debugs are radically different.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Brief PEM State on Show Client Output

To parse through show client and debugs first requires you to understand some Power Entry Module (PEM) states and APF states.

- START—Initial status for new client entry.
- AUTHCHECK—WLAN has an L2 authentication policy to enforce.
- 8021X_REQD—Client must complete 802.1x authentication.
- L2AUTHCOMPLETE—The client has successfully finished the L2 policy. The process can now proceed to L3 policies (address learning, Web auth, and so on). Controller sends the mobility announcement to learn L3 information from other controllers if this is a roaming client in the same

mobility group.
- WEP_REQD—Client must complete WEP authentication.
- DHCP_REQD—Controller learns the L3 address from client, which is done either by ARP request, DHCP request or renew, or by information learned from other controllers in the mobility group. If DHCP Required is marked on the WLAN, only DHCP or mobility information are used.
- WEBAUTH_REQD—Client must complete Web authentication. (L3 policy)
- CENTRAL_WEBAUTH_REQD—Client must complete CWA log in. WLC waits to receive the CoA.
- RUN—Client has successfully completed the required L2 and L3 policies and can now transmit traffic to the network.

The given scenarios show key debug lines for common misconfigurations in wireless setups, which highlights key parameters in **bold**.

Scenario 1: Misconfigured Passphrase for WPA/WPA2 PSK Authentication on Client

<#root>

```
(Cisco Controller) >show client detail 24:77:03:19:fb:70

Client MAC Address............................... 24:77:03:19:fb:70

Client Username ................................. N/A

AP MAC Address................................... ec:c8:82:a4:5b:c0

AP Name.......................................... Shankar_AP_1042


AP radio slot Id................................. 1

Client State..................................... Associated


Client NAC OOB State............................. Access

Wireless LAN Id.................................. 5

Hotspot (802.11u)................................ Not Supported

BSSID............................................ ec:c8:82:a4:5b:cb


Connected For ................................... 0 secs

Channel.......................................... 44

IP Address....................................... Unknown

Gateway Address.................................. Unknown
```

```
Netmask.......................................... Unknown

Association Id................................... 1

Authentication Algorithm......................... Open System

Reason Code...................................... 1

Status Code...................................... 0

Session Timeout.................................. 0

Client CCX version............................... 4

Client E2E version............................... 1

QoS Level........................................ Silver

Avg data Rate.................................... 0

Burst data Rate.................................. 0

Avg Real time data Rate.......................... 0

Burst Real Time data Rate........................ 0

802.1P Priority Tag.............................. 2

CTS Security Group Tag........................... Not Applicable

KTS CAC Capability............................... No

WMM Support...................................... Enabled

  APSD ACs.......................................  BK  BE  VI  VO

Power Save....................................... OFF

Current Rate..................................... m15

Supported Rates.................................. 6.0,9.0,12.0,18.0,24.0,36.0,

    ............................................. 48.0,54.0

Mobility State................................... None

Mobility Move Count.............................. 0

Security Policy Completed........................ No
```

Policy Manager State............................. 8021X_REQD

***This proves client is struggling to clear Layer-2 authentication.
It means we have to move to debug to understand where in L-2 we are failing

```
Policy Manager Rule Created...................... Yes

Audit Session ID................................. none

AAA Role Type.................................... none
```

```
Local Policy Applied............................. none

IPv4 ACL Name.................................... none

FlexConnect ACL Applied Status................... Unavailable

IPv4 ACL Applied Status.......................... Unavailable

IPv6 ACL Name.................................... none

IPv6 ACL Applied Status.......................... Unavailable

Layer2 ACL Name.................................. none

Layer2 ACL Applied Status........................ Unavailable

mDNS Status...................................... Enabled

mDNS Profile Name................................ default-mdns-profile

No. of mDNS Services Advertised.................. 0

Policy Type...................................... WPA2

Authentication Key Management.................... PSK

Encryption Cipher................................ CCMP (AES)

Protected Management Frame ...................... No

Management Frame Protection...................... No

EAP Type......................................... Unknown

Interface........................................ vlan21

VLAN............................................. 21

Quarantine VLAN.................................. 0

Access VLAN...................................... 21

Client Capabilities:

      CF Pollable................................ Not implemented

      CF Poll Request............................ Not implemented

      Short Preamble............................. Not implemented

      PBCC....................................... Not implemented

      Channel Agility............................ Not implemented

      Listen Interval............................ 10

      Fast BSS Transition........................ Not implemented

Client Wifi Direct Capabilities:

      WFD capable................................ No
      Manged WFD capable......................... No
      Cross Connection Capable................... No
      Support Concurrent Operation............... No
Fast BSS Transition Details:
Client Statistics:
      Number of Bytes Received................... 423
      Number of Bytes Sent....................... 429
      Number of Packets Received................. 3
      Number of Packets Sent..................... 4
      Number of Interim-Update Sent.............. 0
      Number of EAP Id Request Msg Timeouts...... 0
      Number of EAP Id Request Msg Failures...... 0
      Number of EAP Request Msg Timeouts......... 0
      Number of EAP Request Msg Failures......... 0
      Number of EAP Key Msg Timeouts............. 0
      Number of EAP Key Msg Failures............. 0
      Number of Data Retries..................... 0
      Number of RTS Retries...................... 0
      Number of Duplicate Received Packets....... 0
      Number of Decrypt Failed Packets........... 0
      Number of Mic Failured Packets............. 0
      Number of Mic Missing Packets.............. 0
      Number of RA Packets Dropped............... 0
      Number of Policy Errors.................... 0
      Radio Signal Strength Indicator............ -18 dBm
      Signal to Noise Ratio...................... 40 dB
Client Rate Limiting Statistics:
      Number of Data Packets Received............ 0
      Number of Data Rx Packets Dropped.......... 0
      Number of Data Bytes Received.............. 0
      Number of Data Rx Bytes Dropped............ 0
      Number of Realtime Packets Received........ 0
      Number of Realtime Rx Packets Dropped...... 0
      Number of Realtime Bytes Received.......... 0
      Number of Realtime Rx Bytes Dropped........ 0
      Number of Data Packets Sent................ 0
      Number of Data Tx Packets Dropped.......... 0
      Number of Data Bytes Sent.................. 0
      Number of Data Tx Bytes Dropped............ 0
      Number of Realtime Packets Sent............ 0
      Number of Realtime Tx Packets Dropped...... 0
      Number of Realtime Bytes Sent.............. 0
      Number of Realtime Tx Bytes Dropped........ 0
Nearby AP Statistics:
      Shankar_AP_1602(slot 0)
        antenna0: 0 secs ago..................... -25 dBm
        antenna1: 0 secs ago..................... -40 dBm
      Shankar_AP_1602(slot 1)
        antenna0: 1 secs ago..................... -41 dBm
        antenna1: 1 secs ago..................... -27 dBm
      Shankar_AP_3502(slot 0)
        antenna0: 0 secs ago..................... -90 dBm
        antenna1: 0 secs ago..................... -83 dBm
      Shankar_AP_1042(slot 0)
        antenna0: 0 secs ago..................... -32 dBm
        antenna1: 0 secs ago..................... -41 dBm
      Shankar_AP_1042(slot 1)
        antenna0: 0 secs ago..................... -50 dBm
        antenna1: 0 secs ago..................... -42 dBm
DNS Server details:
      DNS server IP ............................. 0.0.0.0
      DNS server IP ............................. 0.0.0.0
```

```
Assisted Roaming Prediction List details:



 Client Dhcp Required:     False

Allowed (URL)IP Addresses

-------------------------
```

Debug client analysis:

<#root>

```
(Cisco Controller) >debug client 24:77:03:19:fb:70
```

***apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 Association received from mobile on BSSID 08:cc**

```
*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 Global 200 Clients are allowed to AP radio


*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 Max Client Trap Threshold: 0  cur: 0


*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 Rf profile 600 Clients are allowed to AP wlan


*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 Applying Interface policy on Mobile, role Unas


*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 Re-applying interface policy for client


*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 0.0.0.0 START (0) Changing IPv4 ACL 'none' (AC
*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 0.0.0.0 START (0) Changing IPv6 ACL 'none' (AC
*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 apfApplyWlanPolicy: Apply WLAN Policy over PMI
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 In processSsidIE:4795 setting Central switched
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 In processSsidIE:4798 apVapId = 5 and Split Ac
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Applying site-specific Local Bridging override
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Applying Local Bridging Interface Policy for s
```

```
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 processSsidIE  statusCode is 0 and status is 0
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 processSsidIE  ssid_done_flag is 0 finish_flag
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 STA - rates (8): 140 18 24 36 48 72 96 108 0 0
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 suppRates  statusCode is 0 and gotSuppRatesEle
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Processing RSN IE type 48, length 22 for mobil
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 pemApfDeleteMobileStation2: APF_MS_PEM_WAIT_L2_
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 0.0.0.0 START (0) Deleted mobile LWAPP rule on
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Updated location for station old AP ec:c8:82:a
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Updating AID for REAP AP Client 08:cc:68:67:1f
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 0.0.0.0 START (0) Initializing policy
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 0.0.0.0 START (0) Change state to AUTHCHECK (2

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQ
***Client entering L2 authentication stage

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Central switch is TRUE
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Not Using WMM Compliance code qosCap 00
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP ru
*apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 apfMsAssoStateInc
*apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 apfPemAddUser2 (apf_policy.c:333) Changing sta

*apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 apfPemAddUser2:session timeout forstation 24:7
*apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 Stopping deletion of Mobile Station: (callerId
*apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 Func: apfPemAddUser2, Ms Timeout = 0, Session

*apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 Sending Assoc Response to station on BSSID 08:
*apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 apfProcessAssocReq (apf_80211.c:8292) Changing

*spamApTask3: May 07 17:03:56.065: 24:77:03:19:fb:70 Sent 1x initiate message to multi thread task for
*Dot1x_NW_MsgTask_0: May 07 17:03:56.065: 24:77:03:19:fb:70 Creating a PKC PMKID Cache entry for statio
*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Resetting MSCB PMK Cache Entry 0 for statio
```

```
*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Removing BSSID ec:c8:82:a4:5b:cb from PMKID

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Setting active key cache index 0 ---> 8

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Setting active key cache index 8 ---> 0

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Adding BSSID 08:cc:68:67:1f:fb to PMKID cac

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: New PMKID: (16)


*Dot1x_NW_MsgTask_0: May 07 17:03:56.066:      [0000] d7 57 8e ff 2b 27 01 4e 93 39 0b 1c 1f 46 d2 da


*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Initiating RSN PSK to mobile 24:77:03:19:fb

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 EAP-PARAM Debug - eap-params for Wlan-Id :5

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 dot1x - moving mobile 24:77:03:19:fb:70 int

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 EAPOL Header:

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 00000000: 02 03 00 5f                                      .

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Found an cache entry for BSSID 08:cc:68:67:

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066:
24:77:03:19:fb:70 Found an cache entry for BSSID 08:cc:68:67:1f:fb in PMKID cache at index 0 of station

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: Including PMKID in M1  (16)


*Dot1x_NW_MsgTask_0: May 07 17:03:56.066:      [0000] d7 57 8e ff 2b 27 01 4e 93 39 0b 1c 1f 46 d2 da


*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Starting key exchange to mobile 24:77:03:19:

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Sending EAPOL-Key Message to mobile 24:77:0

   state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Sending EAPOL-Key Message to mobile 24:77:0

   state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Allocating EAP Pkt for retransmission to mo

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 mscb->apfMsLwappLradNhMac = b0:fa:eb:b8:f5:

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70  mscb->apfMsBssid = 08:cc:68:67:1f:f0 mscb-

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70  dot1xcb->snapOrg = 00 00 00 dot1xcb->eapol

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70  mscb->apfMsLwappMwarPort = 5246 mscb->apfM

*Dot1x_NW_MsgTask_0: May 07 17:03:56.069: 24:77:03:19:fb:70 Received EAPOL-Key from mobile 24:77:03:19:
```

```
*Dot1x_NW_MsgTask_0: May 07 17:03:56.069: 24:77:03:19:fb:70 Ignoring invalid EAPOL version (1) in EAPOL

*Dot1x_NW_MsgTask_0: May 07 17:03:56.069: 24:77:03:19:fb:70 Received EAPOL-key in PTK_START state (mess

*Dot1x_NW_MsgTask_0: May 07 17:03:56.069: 24:77:03:19:fb:70 Received EAPOL-key M2 with invalid MIC from

*osapiBsnTimer: May 07 17:03:56.364: 24:77:03:19:fb:70 802.1x 'timeoutEvt' Timer expired for station 24:

 ***!--- MIC error due to wrong preshared key


*dot1xMsgTask: May 07 17:03:56.364: 24:77:03:19:fb:70 Retransmit 1 of EAPOL-Key M1 (length 121) for mobi

*dot1xMsgTask: May 07 17:03:56.364: 24:77:03:19:fb:70 mscb->apfMsLwappLradNhMac = b0:fa:eb:b8:f5:12 mscb

*dot1xMsgTask: May 07 17:03:56.364: 24:77:03:19:fb:70  mscb->apfMsBssid = 08:cc:68:67:1f:f0 mscb->apfMsA

*dot1xMsgTask: May 07 17:03:56.365: 24:77:03:19:fb:70  dot1xcb->snapOrg = 00 00 00 dot1xcb->eapolWepBit

*dot1xMsgTask: May 07 17:03:56.365: 24:77:03:19:fb:70  mscb->apfMsLwappMwarPort = 5246 mscb->apfMsLwapp

*Dot1x_NW_MsgTask_0: May 07 17:03:56.366: 24:77:03:19:fb:70 Received EAPOL-Key from mobile 24:77:03:19:

*Dot1x_NW_MsgTask_0: May 07 17:03:56.366: 24:77:03:19:fb:70 Ignoring invalid EAPOL version (1) in EAPOL

*Dot1x_NW_MsgTask_0: May 07 17:03:56.366: 24:77:03:19:fb:70 Received EAPOL-key in PTK_START state (mess

*Dot1x_NW_MsgTask_0: May 07 17:03:56.366: 24:77:03:19:fb:70 Received EAPOL-key M2 with invalid MIC from

*osapiBsnTimer: May 07 17:03:56.764: 24:77:03:19:fb:70 802.1x 'timeoutEvt' Timer expired for station 24:

 ***!--- MIC error due to wrong preshared key
```

Conclusion

Though timeoutEvt for M2 key could also be due to driver/NIC errors, one of the most common issues is a user who enters incorrect credentials for PSK password (missed case sensitive/ special characters, and so on) and is unable to connect.

Scenario 2: Wireless Phone Handset (792x/9971) Fails to Associate with Wireless "Leaves Service Area"

Reference: 7925G Handsets Failing Association to AP - Call Failed: TSPEC QOS Policy does not Match

Topology

WLAN with Cisco Unified Wireless IP Phones.

Problem Details

AIR-CT5508-50-K9 // upgraded firmware for phones and wireless controller does not accept phone registrations.

Debugs and logs:

<#root>

```
apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Association received from mobile on AP 3x:xx:cx:9

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx 0.0.0.0 START (0) Changing IPv4 ACL 'none' (ACL

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx 0.0.0.0 START (0) Changing IPv6 ACL 'none' (ACL

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Applying site-specific Local Bridging override

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Applying Local Bridging Interface Policy for st

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx processSsidIE  statusCode is 0 and status is 0

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx processSsidIE  ssid_done_flag is 0 finish_flag

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx STA - rates (4): 130 132 139 150 0 0 0 0 0 0 0

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx suppRates  statusCode is 0 and gotSuppRatesElem

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx STA - rates (12): 130 132 139 150 12 18 24 36 4

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx extSuppRates  statusCode is 0 and gotExtSuppRat

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Processing RSN IE type 48, length 22 for mobile

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx CCKM: Mobile is using CCKM

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Received RSN IE with 0 PMKIDs from mobile 1x:xx

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Setting active key cache index 8 ---> 8

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx unsetting PmkIdValidatedByAp

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Sending Assoc Response to station on BSSID 3x:x

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Scheduling deletion of Mobile Station:  (caller
VoIP Call Failure: '1x:xx:1x:xx:xx:xx' client, detected by 'xx-xx-xx' AP on radio type '802.11b/g'. Rea

.
***Means platinum QoS was not configured on WLAN

1x:xx PM


Client Excluded: MACAddress:1x:xx:1x:xx:xx:xx Base Radio MAC :3x:xx:cx:9x:x0:x0 Slot: 1 User Name: dwpv
```

Conclusion

Debug on the WLC shows that the 7925G fails association as the AP returns an Association status code of 201.

This is due to a Traffic SPECification (TSPEC) request from the handset refusal due to the WLAN configuration. The WLAN 7925G that attempts to connect is configured with a QoS profile of Silver (UP 0,3), rather than Platinum (UP 6,7) as required. This leads to a TSPEC mismatch for voice traffic/action frame exchange from the handset by the WLAN, and ultimately a rejection from the AP.

Create a new WLAN with a QoS profile of Platinum specifically for the 7925G handsets and configured as per established best practices, and as defined in the 7925G Deployment Guide:

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Deployment Guide

Once configured correctly, the issue is resolved.

Scenario 3: Client Configured for WPA but AP Configured only for WPA2

debug client <mac addr>:

<#root>

```
Wed May 7 10:51:37 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile

    Station:  (callerId: 23) in 5 seconds

Wed May 7 10:51:37 2014: xx.xx.xx.xx.xx.xx apfProcessProbeReq

    (apf_80211.c:4057) Changing state for mobile xx.xx.xx.xx.xx.xx on AP


from Idle to Probe



***Controller adds the new client, moving into probing status



Wed May 7 10:51:37 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile

    Station:  (callerId: 24) in 5 seconds

Wed May 7 10:51:38 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile

    Station:  (callerId: 24) in 5 seconds

Wed May 7 10:51:38 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile

    Station:  (callerId: 24) in 5 seconds


***AP is reporting probe activity every 500 ms as configured
```

```
Wed May 7 10:51:41 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile

    Station:  (callerId: 24) in 5 seconds

Wed May 7 10:51:41 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile

    Station:  (callerId: 24) in 5 seconds

Wed May 7 10:51:41 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile

    Station:  (callerId: 24) in 5 seconds

Wed May 7 10:51:41 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile

    Station:  (callerId: 24) in 5 seconds

Wed May 7 10:51:44 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile

    Station:  (callerId: 24) in 5 seconds

Wed May 7 10:51:44 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile

    Station:  (callerId: 24) in 5 seconds

Wed May 7 10:51:44 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile

    Station:  (callerId: 24) in 5 seconds

Wed May 7 10:51:44 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile

    Station:  (callerId: 24) in 5 seconds

Wed May 7 10:51:49 2014: xx.xx.xx.xx.xx.xx apfMsExpireCallback (apf_ms.c:433)

    Expiring Mobile!

Wed May 7 10:51:49 2014: xx.xx.xx.xx.xx.xx 0.0.0.0 START (0) Deleted mobile

    LWAPP rule on AP []

Wed May 7 10:51:49 2014: xx.xx.xx.xx.xx.xx Deleting mobile on AP

    (0)



***After 5 seconds of inactivity, client is deleted, never moved into authentication or association phas
```

Scenario 4: Parse AAA Return or Response Codes

Required debugs to RUN to collect the expected logs:

(Cisco Controller) > **debug mac addr <mac>**

(Cisco Controller) > **debug aaa events enable**

(OR)

(Cisco Controller) > **debug client <mac>**

(Cisco Controller) > **debug aaa events enable**

(Cisco Controller) > **debug aaa errors enable**

AAA connectivity failure generates an SNMP trap, if traps are enabled.

Example debug output <snipped>:

<#root>

```
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 Invalid RADIUS message authenticator for
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 RADIUS message verification failed from
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 Returning AAA Error 'Authentication Fail
*radiusTransportThread: Mar 26 17:54:58.054: AuthorizationResponse: 0x4259f944
```

Returning AAA Error 'Success' (0) for mobile

Successful Authentication happened, AAA returns access-accept prior to Success (0) to confirm the same.

Returning AAA Error 'Out of Memory' (-2) for mobile

***it's the rare reason. Cisco bug ID CSCud12582 ***Proc

Returning AAA Error 'Authentication Failed' (-4) for mobile

***its the most common reason seen

Possible Reasons:

1. Invalid user account and/or password.
2. Computer not a member of domain, issue on AD side.

3. Certificate services do not work properly.
4. Server Certificate expired or not in use.
5. RADIUS incorrectly configured.
6. Access key incorrectly entered - it IS case sensitive (and so is the SSID).
7. Update Microsoft patches.
8. EAP timers.
9. Incorrect EAP method configured on client/server.
10. Client certificate is expired or not in use.

Return AAA Error Timeout (-5) for Mobile
AAA Server Unreachable, followed by client deauth.

Example:

<#root>

```
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Max retransmission of Access-Request (id 100) to 209.165.20
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 [Error] Client requested no retries for mobile 00:13:CE:1A:

Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Returning AAA Error 'Timeout' (-5) for mobile 00:13:ce:1a:92


Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Processing AAA Error 'Timeout' (-5) for mobile 00:13:ce:1a:9
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Sent Deauthenticate to mobile on BSSID 00:0b:85:76:d3:e0 slo

Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Scheduling deletion of Mobile Station: (callerId: 65) in 10
```

Return AAA Error Internal Error (-6) for Mobile

Attribute mismatch. AAA sends incorrect/inappropriate attribute (wrong length) that is not understood/compatible with WLC. WLC sends Deauth message, followed by internal error message.
Example: Cisco bug ID CSCum83894 AAA Internal Error and auth fail with unknown attributes in access accept.

Example:

```
*radiusTransportThread: Feb 21 12:14:36.109: Aborting ATTR processing 599 (avp 26/6)
*radiusTransportThread: Feb 21 12:14:36.109: 40:f0:2f:11:a9:fd Invalid RADIUS response received from se
*radiusTransportThread: Feb 21 12:14:36.109: 40:f0:2f:11:a9:fd [Error] Client requested no retries for m
*radiusTransportThread: Feb 21 12:14:36.109: 40:f0:2f:11:a9:fd Returning AAA Error 'Internal Error' (-6)
*radiusTransportThread: Feb 21 12:14:36.109:
resultCode.................................-6
*Dot1x_NW_MsgTask_5: Feb 21 12:14:36.109: 40:f0:2f:11:a9:fd Processing AAA Error 'Internal Error' (-6) f
```

Returns AAA Error No Server (-7) for mobile.
Radius is not properly configured and/or unsupported configuration in use.

Example:

```
*Jun 22 20:32:10.229: 00:21:e9:57:3c:bf Returning AAA Error 'No Server' (-7) for mobile 00:21:e9:57:3c:
*Jun 22 20:32:10.229: AuthorizationResponse: 0x1eebb3ec
```

Scenario 5: Client Fails to Associate to AP

Debug used:

debug client <mac addr>

Logs to parse:

Sending Assoc Response to station on BSSID 00:26:cb:94:44:c0 (status 0) ApVapId 1 Slot 0

- Slot 0 = B/G(2.4) Radio
- Slot 1 = A(5) Radio
- Sends Assoc Response Status 0 = Success

Anything other than Status 0 is Failure.

Common Association Response status codes can be found at: 802.11 Association Status, 802.11 Deauth Reason Codes

Scenario 6: Client Disassociation Due to Idle Timeout

Debug used:

debug client <mac addr>

Logs to parse

Received Idle-Timeout from AP 00:26:cb:94:44:c0, slot 0 for STA 00:1e:8c:0f:a4:57

apfMsDeleteByMscb Scheduling mobile for deletion with deleteReason 4, reasonCode 4

Scheduling deletion of Mobile Station: (callerId: 30) in 1 seconds

apfMsExpireCallback (apf_ms.c:608) Expiring Mobile!

Sent Deauthenticate to mobile on BSSID 00:26:cb:94:44:c0 slot 0(caller apf_ms.c:5094)

Conditions

Occurs after no traffic received from Client.

Default Duration is 300 seconds.

Workaround

Increase Idle Timeout either globally from WLC GUI>>Controller>>General, or per WLAN from WLC **GUI>WLAN>ID>>Advanced**.

Scenario 7: Client Disassociation Due to Session Timeout

Debug used:

debug client <mac addr>

Logs to parse:

```
apfMsExpireCallback (apf_ms.c:608) Expiring Mobile!

apfMsExpireMobileStation (apf_ms.c:5009) Changing state for mobile 00:1e:8c:0f:a4:57 on

               AP 00:26:cb:94:44:c0 from Associated to Disassociated

Scheduling deletion of Mobile Station:  (callerId: 45) in 10 seconds

apfMsExpireCallback (apf_ms.c:608) Expiring Mobile!

Sent Deauthenticate to mobile on BSSID 00:26:cb:94:44:c0 slot 0(caller apf_ms.c:5094)
```

Conditions

Occurs at scheduled duration (default 1800 seconds).

It forces the WEBAUTH user to WEBAUTH again.

Workaround

Increase or disable session timeout per WLAN from WLC **GUI>WLAN>ID>Advanced.**

Scenario 8: Client Disassociation Due to WLAN changes

Debug used:

debug client <mac addr>

Log to parse:

```
apfSendDisAssocMsgDebug (apf_80211.c:1855) Changing state for mobile

               00:1e:8c:0f:a4:57 on AP 00:26:cb:94:44:c0 from Associated to Disassociated

Sent Disassociate to mobile on AP 00:26:cb:94:44:c0-0 (reason 1, caller apf_ms.c:4983)

Sent Deauthenticate to mobile on BSSID 00:26:cb:94:44:c0 slot 0(caller apf_ms.c:5094)
```

Conditions

To modify a WLAN in any way disables and re-enables WLAN.

Workaround

This is expected behavior. When there are WLAN changes made, clients disassociate and re-associate.

Scenario 9: Client Disassociation Due to Manual Deletion from WLC

Debug used:

debug client <mac addr>

Log to parse:

```
apfMsDeleteByMscb Scheduling mobile for deletion with deleteReason 6, reasonCode 1

Scheduling deletion of Mobile Station:  (callerId: 30) in 1 seconds

apfMsExpireCallback (apf_ms.c:608) Expiring Mobile!

apfMsExpireMobileStation (apf_ms.c:5009) Changing state for mobile 00:1e:8c:0f:a4:57 on

                AP 00:26:cb:94:44:c0 from Associated to Disassociated

Sent Deauthenticate to mobile on BSSID 00:26:cb:94:44:c0 slot 0(caller apf_ms.c:5094)
```

Conditions

From GUI: Remove Client

From CLI: **config client deauthenticate <mac address>**

Scenario 10: Client Disassociation Due to Authentication Timeout

Debug used:

debug client <mac addr>

Log to parse:

```
Retransmit failure for EAPOL-Key M3 to mobile 00:1e:8c:0f:a4:57, retransmit count 3, mscb deauth count

Sent Deauthenticate to mobile on BSSID 00:26:cb:94:44:c0 slot 0(caller 1x_ptsm.c:534)
```

Conditions

Authentication or Key Exchange max-retransmissions reached.

Workaround

Check/update client driver, security config, certificates, and so on.

Scenario 11: Client Disassociation Due to AP Radio Reset (Power/Channel)

Debug used:

debug client <mac addr>

Log to parse:

```
Cleaning up state for STA 00:1e:8c:0f:a4:57 due to event for AP 00:26:cb:94:44:c0(0)

apfSendDisAssocMsgDebug (apf_80211.c:1855) Changing state for mobile

                00:1e:8c:0f:a4:57 on AP 00:26:cb:94:44:c0 from Associated to Disassociated

Sent Disassociate to mobile on AP 00:26:cb:94:44:c0-0 (reason 1, caller apf_ms.c:4983)
```

Conditions

AP disassociates clients, but WLC does not delete entry.

Workaround

Expected behavior.

Scenario 12: Symantec Client Issues with 802.1X "timeoutEvt"

Issue

Clients that run Symantec software disassociate with message 802.1X timeoutEvt. Timer expired for the station and for message = M3

EAP/Eapol process does not get completed, irrespective of A/G radio used on the intel/Broadcom card. No issue when it is used wep, wpa-psk.

Conditions

WLC code does not matter.

APs - all model - All on local mode.
wlan 3 - WPA2+802.1X PEAP + mshcapv2
SSID is broadcast.

RADIUS server nps 2008.
Symantec antivirus software is installed on all the PCs.

Use Asus, Broadcom, Intel - win7, win-xp.

Affected OS - Windows 7 and xp

Affected Wireless adapter - Intel(6205) and Broadcom

Affected Driver/Supplicant - 15.2.0.19, use Native Supplicant.

Fix/Workaround

Disable Symantec Network Protection and Firewall on win7 and xp. It is a Symantec issue with Win 7 and XP OS.

Debug output:

```
*dot1xMsgTask: Apr 12 11:45:39.335: 84:3a:4b:7a:d5:ac Retransmit 1 of EAPOL-Key M3 (length 155) for mob
*osapiBsnTimer: Apr 12 11:45:44.336: 84:3a:4b:7a:d5:ac 802.1x 'timeoutEvt' Timer expired for station 84
*dot1xMsgTask: Apr 12 11:45:44.336: 84:3a:4b:7a:d5:ac Retransmit 2 of EAPOL-Key M3 (length 155) for mob
*osapiBsnTimer: Apr 12 11:45:49.336: 84:3a:4b:7a:d5:ac 802.1x 'timeoutEvt' Timer expired for station 84
*dot1xMsgTask: Apr 12 11:45:49.336: 84:3a:4b:7a:d5:ac Retransmit 3 of EAPOL-Key M3 (length 155) for mob
*osapiBsnTimer: Apr 12 11:45:54.336: 84:3a:4b:7a:d5:ac 802.1x 'timeoutEvt' Timer expired for station 84
*dot1xMsgTask: Apr 12 11:45:54.337: 84:3a:4b:7a:d5:ac Retransmit 4 of EAPOL-Key M3 (length 155) for mob
*osapiBsnTimer: Apr 12 11:45:59.336: 84:3a:4b:7a:d5:ac 802.1x 'timeoutEvt' Timer expired for station 84
*dot1xMsgTask: Apr 12 11:45:59.336: 84:3a:4b:7a:d5:ac Retransmit failure for EAPOL-Key M3 to mobile 84:
*dot1xMsgTask: Apr 12 11:45:59.338: 84:3a:4b:7a:d5:ac Sent Deauthenticate to mobile on BSSID c8:f9:f9:8
```

Note: There is a syndrome in 15.2 (also seen in earlier versions) that goes like:
-client gets M1 from AP
-client sends M2
-client gets M3 from AP
-client plumbs the new pairwise key before it sends out M4

- Client transmits the M4 encrypted with the new key AP, drops the M4 message as a "decrypt error".

- WLC debug client shows that you time out on M3 retransmissions. Evidently, this is a problem between Microsoft and Symantec, not Intel-specific. The workaround is to remove Symantec.

- This is really a bug that is probably in Windows, triggered by Symantec. Tweak of the EAP timer does not fix this issue.

- Regarding this issue, Cisco TAC forwards the affected users to Symantec and Microsoft.

Scenario 13: Air Print Service does not Show up for Clients with mDNS that Snoop Turned On

Client not able to see devices that provides AirPrint service on Apple handheld client devices when mDNS snoop is turned on.

Conditions

5508 WLC with 7.6.100.0.
With mDNS snoop enabled, you have the devices that provide AirPrint services listed under the services section on the WLC.
The respective mDNS profile was mapped correctly to the WLAN and the Interface.
Still unable able to see the AirPrint devices on the client.

Debug used:

debug client <mac addr>

debug mdns all enable

```
*Bonjour_Msg_Task: Apr 15 15:29:35.640: b0:65:bd:df:f8:71 Query Service Name: _universal._sub._ipp._tcp
*Bonjour_Msg_Task: Apr 15 15:29:35.640: qNameStr:_universal._sub._ipp._tcp.local., bonjServiceNameStr:_
*Bonjour_Msg_Task: Apr 15 15:29:35.640: Service Name : HP_Photosmart_Printer_1  Service String : _unive
*Bonjour_Msg_Task: Apr 15 15:29:35.640: b0:65:bd:df:f8:71 Service:_universal._sub._ipp._tcp.local. is s
*Bonjour_Msg_Task: Apr 15 15:29:35.640: processBonjourPacket : 986 AP-MAC = C8:4C:75:D1:77:20 has ap-gr
*Bonjour_Msg_Task: Apr 15 15:29:35.640: Sending Bonjour Response
*Bonjour_Msg_Task: Apr 15 15:29:35.640: Service Provider Name: _dns-sd._udp.YVG.local., Msal Service Na
*Bonjour_Msg_Task: Apr 15 15:29:35.640:  Sending Query Response bonjSpNameStr: _dns-sd._udp.YVG.local.,
*Bonjour_Msg_Task: Apr 15 15:29:35.640:  vlanId : 909, allvlan : 0, isMcast : 1, toSta : 1
*Bonjour_Msg_Task: Apr 15 15:29:35.640: b0:65:bd:df:f8:71 Successfully sent response for service: _univ

*Bonjour_Process_Task: Apr 15 15:29:35.641: Inside buildBonjourQueryResponsePld, available_len =1366
*Bonjour_Process_Task: Apr 15 15:29:35.641: Not able to attach any record
*Bonjour_Process_Task: Apr 15 15:29:35.641: Error building the Bonjour Packet !!
```

Explanation:

The client would request for _universal._sub._ipps._tcp.local or _universal._sub._ipp._tcp.local instead of **_ipp._tcp.local** or _ipp._tcp.local string.
So the added AirPrint service would not work. It was identified and the requested service string to be mapped to HP_Photosmart_Printer_1.
The same service was added in the profile mapped to the WLAN and still there was no service listed for the device.

It was found that due to the domain name appended and the client query for dns-sd._udp.YVG **local** with the domain name appended, the WLC was not able to process the Bonjour packet as dns-sd._udp.YVG.local does not exist in the database.

Identified the given enhancement bug with regard to the same - Cisco bug ID CSCuj32157.

Workaround

The only work around was to disable DHCP option 15 (Domain name) or to remove the Domain name from the client.

Scenario 14: Apple iOS Client "Unable to Join the Network" Due to Disabled Fast SSID Change

Conditions

Most Apple iOS devices have issues to move from one WLAN to another on the same Cisco WLC with the default fast SSID change disabled.

The setting causes the controller to deauthenticate the client from the WLAN that exists once the client attempts to associate to another.

The typical result is an "Unable to Join the Network" message on the iOS device.

Show client

(jk-2504-116) >**show network summary**

<snip>

Fast SSID Change .... Disabled

Debug used:

<#root>

```
(jk-2504-116) >

debug client 1c:e6:2b:cd:da:9d




(jk-2504-116) >

*apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Association received from mobile on BSSID 00:2

***Apple Client initiating switch from one wlan to another.

*apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Global 200 Clients are allowed to AP radio



*apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Max Client Trap Threshold: 0  cur: 1



*apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Rf profile 600 Clients are allowed to AP wlan



*apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Deleting client immediately since WLAN has char

*apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Scheduling deletion of Mobile Station:  (calle

*osapiBsnTimer: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d apfMsExpireCallback (apf_ms.c:625) Expiring Mobi

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d apfMsExpireMobileStation (apf_ms.c:6632) Changi
```

```
*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Sent Deauthenticate to mobile on BSSID 00:21:a0:

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Found an cache entry for BSSID 00:21:a0:e3:fd:bf

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Removing BSSID 00:21:a0:e3:fd:bf from PMKID cac

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Resetting MSCB PMK Cache Entry 0 for station 1c

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Setting active key cache index 0 ---> 8

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Deleting the PMK cache when de-authenticating t

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Global PMK Cache deletion failed.

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d apfMsAssoStateDec

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d apfMsExpireMobileStation (apf_ms.c:6764) Changi


*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d pemApfDeleteMobileStation2: APF_MS_PEM_WAIT_L2_

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d 192.0.2.254 START (0) Deleted mobile LWAPP rule

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d Deleting mobile on AP 00:21:a0:e3:fd:b0(1)


*pemReceiveTask: Jan 30 21:33:15.377: 1c:e6:2b:cd:da:9d 192.0.2.254 Removed NPU entry.


*apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Adding mobile on LWAPP AP 00:21:a0:e3:fd:b0(1)
***No client activity for > 7 sec due to fast-ssid change disabled

*apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Association received from mobile on BSSID 00:2

*apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Global 200 Clients are allowed to AP radio

 <Snip>


 *apfMsConnTask_7: Jan 30 21:33:23.891: 1c:e6:2b:cd:da:9d Sending Assoc Response to station on BSSID 00:


*apfMsConnTask_7: Jan 30 21:33:23.892: 1c:e6:2b:cd:da:9d apfProcessAssocReq (apf_80211.c:8292) Changing
```

Workaround

Enable fast-ssid change from WLC GUI > Controller>General.

Scenario 15: Successful Client LDAP Association

Secure LDAP helps to secure the connection between the controller and LDAP server that uses TLS. This feature is supported with controller software version 7.6 and higher.

There are two types of queries that can be sent by the controller to the LDAP server:

1. Anonymous

In this type, the controller sends an authentication request to the LDAP server when a client needs to get authenticated. The LDAP server responds with the result of the query. At the time of this exchange, all the information that includes the client username/password is sent in clear text. The LDAP server responds to a query from anyone, as long as the bind username/password are added.

2. Authenticated

In this type, the controller is configured with a username and password which it uses to authenticate itself with the LDAP server. The password is encrypted with MD5 SASL and is sent to the LDAP server at the time of the authentication process. This helps the LDAP server correctly identify the source of the authentication requests. However, even though the identity of the controller is protected, the client details are sent in clear text.

The real need for LDAP over TLS came due to the security vulnerability posed by both of these two types where the client authentication data and the rest of the transaction happens in the clear.

Requirements

WLC runs software version 7.6 and higher.

Microsoft server uses LDAP.

Debug used:

debug aaa ldap enable

```
*LDAP DB Task 1: Feb 06 12:28:12.912: ldapAuthRequest [1] called lcapi_query base="CN=Users,DC=gceaaa,DC
*LDAP DB Task 1: Feb 06 12:28:12.912: Attempting user bind with username CN=Ishaan,CN=Users,DC=gceaaa,DC
*LDAP DB Task 1: Feb 06 12:28:12.914: LDAP ATTR> dn = CN=Ishaan,CN=Users,DC=gceaaa,DC=com (size 35)

*LDAP DB Task 1: Feb 06 12:28:12.914: Handling LDAP response Success //indicates passed LDAP auth.
```

Scenario 16: Client Authentication Failed on LDAP

Debug used:

debug aaa ldap enable

```
*LDAP DB Task 1: Feb 07 17:19:46.535: LDAP_CLIENT: Received no referrals in search result msg
*LDAP DB Task 1: Feb 07 17:19:46.535: LDAP_CLIENT: Received 1 attributes in search result msg
*LDAP DB Task 1: Feb 07 17:19:46.535: ldapAuthRequest [1] called lcapi_query base="CN=Users,DC=gceaaa,DC
*LDAP DB Task 1: Feb 07 17:19:46.535: Handling LDAP response Authentication Failed //Failed auth
*LDAP DB Task 1: Feb 07 17:19:46.536: Authenticated bind : Closing the binded session
```

Workaround

Check LDAP server for reject reasons.

Scenario 17: Client Association Issues Due to LDAP Misconfigured on WLC

Debug used:

debug aaa ldap enable

```
*LDAP DB Task 1: Feb 07 17:21:26.710: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
*LDAP DB Task 1: Feb 07 17:21:26.712: ldapInitAndBind [1] configured Method Authenticated lcapi_bind (r
*LDAP DB Task 1: Feb 07 17:21:26.787: ldapClose [1] called lcapi_close (rc = 0 - Success)
*LDAP DB Task 1: Feb 07 17:21:26.787: LDAP server 1 changed state to IDLE
*LDAP DB Task 1: Feb 07 17:21:26.787: LDAP server 1 changed state to ERROR
*LDAP DB Task 1: Feb 07 17:21:26.787: Handling LDAP response Internal Error
```

Workaround

Verify credentials across client/WLC and LDAP server.

Scenario 18: Client Association Issues when LDAP Server is Unreachable

Debug used:

debug aaa ldap enable

```
*LDAP DB Task 2: Feb 07 17:26:45.874: ldapInitAndBind [2] configured Method Anonymous lcapi_bind (rc =
*LDAP DB Task 2: Feb 07 17:26:45.874: ldapClose [2] called lcapi_close (rc = 0 - Success)
*LDAP DB Task 2: Feb 07 17:26:45.875: LDAP server 2 changed state to IDLE
*LDAP DB Task 2: Feb 07 17:26:45.875: LDAP server 2 changed state to ERROR
*LDAP DB Task 2: Feb 07 17:26:45.875: Handling LDAP response Internal Error
```

Workaround

Check WLC and LDAP server network connectivity issues.

Scenario 19: Apple Client Roaming Issues Due to Missing Sticky Roaming Configuration

Conditions

AIR-CT5508-K9 / 7.4.100.0

Apple devices disconnect from a wireless network that uses:

- WPA2 Policy
- WPA2 Encryption AES
- Authentication 802.1X Enabled

Authentication and Authorization by Cisco ISE.

Apple devices periodically disconnect from the broadcast SSID. An example is an iPhone that drops while another phone in the same location remains connected. Therefore, this occurs randomly (time and phone).

Laptop clients with no issues. They connect to the same SSID.

This issue happens during normal operation, with no roaming and no standby mode.

The WLAN already has removed all possible settings that could cause issues (aironet ext).

Debug used:

debug client <mac addr>

<#root>

```
*apfMsConnTask_5: Jun 11 16:12:56.342: f0:d1:a9:bb:2d:fa Received RSN IE with 0 PMKIDs from mobile f0:d1

***At 16:12:56 in the debugs we see a client re-association. From there the AP is expecting the client t
***At this point it does not!  From the above message the AP/WLC didn’t receive a PMKID from the iPhone
***This is kind of expected from this type of client.
***Apple devices do not use the opportunistic key caching which allows clients to use the SAME PMKID at
***Apple devices use a key cache method of Sticky Key Caching.
***This in turn means that the client has to build a PMKID at EACH AP in order to successfully roam to t
***As we can see the client did not present a PMKID to use so we sent it through layer 2 security/EAP ag
***The client then hits a snag in the EAP process where the client fails to respond to the EAP ID or rec

*dot1xMsgTask: Jun 11 16:12:56.345: f0:d1:a9:bb:2d:fa Sending EAP-Request/Identity to mobile f0:d1:a9:bb
*osapiBsnTimer: Jun 11 16:13:26.288: f0:d1:a9:bb:2d:fa 802.1x 'txWhen' Timer expired for station f0:d1:a

***After this snag the client is allowed back onto the network all in approx. 1.5 seconds.
***This is going to be normal and EXPECTED behavior currently with Sticky key cache clients.
```

Workaround

What you can do now for customers that have Sticky Key Caching (SKC) clients and also have WLC code 7.2 and higher, is enable roam support for SKC. By default, the WLC only supports Opportunistic Key Caching (OKC). In order to allow the client to use its old PMKIDs that it generated at each AP, you have to enable it by the WLC CLI.

config wlan security wpa wpa2 cache sticky enable <1>

Please keep in mind this does not improve initial roams due to the nature of SKC; however, it improves subsequent roams to the same APs (up to 8 by the book). Imagine a walk down a hallway with 8 APs. The first walkthrough consists of full associations at each AP with about a 1–2 second lag. When you reach the end and walk back, the client presents 8 unique PMKIDs as it moves back to the same associations.

APs do not have to go through a full authentication if SKC support is enabled. This removes the lag and the client appears to stay connected.

Scenario 20: Verify Fast-Secure-Roaming (FSR) with CCKM

802.11 WLAN Roaming and Fast-Secure Roaming on CUWN

Debug used:

debug client <mac addr>

<#root>

```
*apfMsConnTask_2: Jun 25 15:43:33.749: 00:40:96:b7:ab:5c

CCKM: Received REASSOC REQ IE


*apfMsConnTask_2: Jun 25 15:43:33.749: 00:40:96:b7:ab:5c

Reassociation received from mobile on BSSID  84:78:ac:f0:2a:93

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c

Processing WPA IE type 221, length 22 for mobile  00:40:96:b7:ab:5c
*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c


CCKM: Mobile is using CCKM

***The Reassociation Request is received from the client, which provides the CCKM information needed in

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c Setting active key cache index 0 ---> 8

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c CCKM: Processing REASSOC REQ IE

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c

 CCKM: using HMAC MD5 to compute MIC

 ***WLC computes the MIC used for this CCKM fast-roaming      exchange.

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c CCKM: Received a valid REASSOC REQ IE

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c

CCKM: Initializing PMK cache entry with a new PTK

***The new PTK is derived.

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c Setting active key cache index 8 ---> 8

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c Setting active key cache index 8 ---> 8

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c Setting active key cache index 8 ---> 0

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c

Creating a PKC PMKID Cache entry for station   00:40:96:b7:ab:5c (RSN 0) on BSSID 84:78:ac:f0:2a:93

***The new PMKID cache entry is created for this new      AP-to-client association.
```

```
*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c CCKM: using HMAC MD5 to compute MIC
*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c Including CCKM Response IE (length 62) in Asso
*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c

Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:93   (status 0) ApVapId 4 Slot 0

***The Reassociation Response is sent from the WLC/AP to   the client, which includes the CCKM informat

*dot1xMsgTask: Jun 25 15:43:33.757: 00:40:96:b7:ab:5c


Skipping EAP-Success to mobile 00:40:96:b7:ab:5c

***EAP is skipped due to the fast roaming, and CCKM does not require further key handshakes. The client
```

As shown, fast-secure roaming is performed to avoid the EAP authentication frames and even more 4-Way handshakes, because the new encryption keys are still derived, but based on the CCKM negotiation scheme. This is completed with the roaming reassociation frames and the information previously cached by the client and the WLC.

Scenario 21: Verify Fast-Secure-Roaming (FSR) with WPA2 PMKID Cache

Debug used:

debug client <mac addr>

<#root>

```
*apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32

 Reassociation received from mobile on BSSID 84:78:ac:f0:68:d2

***This is the Reassociation Request from the client.

*apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32

Processing RSN IE type 48, length 38 for mobile ec:85:2f:15:39:32

***The WLC/AP finds an Information Element that claims PMKID Caching support on the Association request

*apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32

Received RSN IE with 1 PMKIDs from mobile ec:85:2f:15:39:32

***The Reassociation Request from the client comes with one PMKID.

*apfMsConnTask_0: Jun 22 00:26:40.787: Received PMKID:  (16)
*apfMsConnTask_0: Jun 22 00:26:40.788: [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5
***This is the PMKID that is received.

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32

Searching for PMKID in MSCB PMKID cache for mobile ec:85:2f:15:39:32

***WLC searches for a matching PMKID on the database.

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32 Found an cache entry for BSSID 84:78:ac:f0:68:

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
```

```
 Found a valid PMKID in the MSCB PMKID cache for mobile ec:85:2f:15:39:32

***The WLC validates the PMKID provided by the client, and confirms that it has a valid PMK cache for t

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32 Setting active key cache index 1 ---> 0

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32

 Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d2(status 0) ApVapId 3 Slot 0

***The Reassociation Response is sent to the client, which validates the fast-roam with SKC.

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32

Initiating RSN with existing PMK to mobile ec:85:2f:15:39:32

***WLC initiates a Robust Secure Network association with this client-and-AP pair based on the cached P

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32 Skipping EAP-Success to mobile ec:85:2f:15:39:32

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32 Found an cache entry for BSSID 84:78:ac:f0:68:d2

*dot1xMsgTask: Jun 22 00:26:40.795:

Including PMKID in M1(16)

***The hashed PMKID is included on the Message-1 of the WPA/WPA2 4-Way handshake.

*dot1xMsgTask: Jun 22 00:26:40.795: [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5
***The PMKID is hashed. The next messages are the same WPA/WPA2 4-Way handshake messages described thus

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32 Sending EAPOL-Key Message to mobile ec:85:2f:15:3

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.811: ec:85:2f:15:39:32 Received EAPOL-Key from mobile ec:85:2f:15:

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812: ec:85:2f:15:39:32 Received EAPOL-key in PTK_START state (mess

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812: ec:85:2f:15:39:32 PMK: Sending cache add

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812: ec:85:2f:15:39:32 Sending EAPOL-Key Message to mobile ec:85:2

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.820: ec:85:2f:15:39:32 Received EAPOL-Key from mobile ec:85:2f:15:

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.820: ec:85:2f:15:39:32 Received EAPOL-key in PTKINITNEGOTIATING st
```

Scenario 22: Verify Fast-Secure Roaming with Proactive Key Cache

Debug used:

debug client <mac addr>

<#root>

```
*apfMsConnTask_2: Jun 21 21:48:50.562: 00:40:96:b7:ab:5c

Reassociation received from mobile on BSSID 84:78:ac:f0:2a:92

***This is the Reassociation Request from the client.

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Processing RSN IE type 48, length 38 for mobil
```

```
***The WLC/AP finds and Information Element that claims PMKID Caching support on the Association reques

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Received RSN IE with 1 PMKIDs from mobile 00:4
***The Reassociation Request from the client comes with one PMKID.

*apfMsConnTask_2: Jun 21 21:48:50.563:Received PMKID:  (16)

*apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Searching for PMKID in MSCB PMKID cache for mo
*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c No valid PMKID found in the MSCB PMKID cache f
***As the client has never authenticated with this new AP, the WLC cannot find a valid PMKID to match t
***However, since the client performs PKC/OKC and not SKC (as per the following messages), the WLC comp

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Trying to compute a PMKID from MSCB PMK cache 

*apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: Find PMK in cache: BSSID =  (6)
*apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 84 78 ac f0 2a 90
*apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: Find PMK in cache: realAA =  (6)
*apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 84 78 ac f0 2a 92
*apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: Find PMK in cache: PMKID =  (16)
*apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9
*apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: AA (6)
*apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 84 78 ac f0 2a 92
*apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: SPA (6)
*apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 00 40 96 b7 ab 5c
*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Adding BSSID 84:78:ac:f0:2a:92 to PMKID cache 
*apfMsConnTask_2: Jun 21 21:48:50.563: New PMKID: (16)
*apfMsConnTask_2: Jun 21 21:48:50.563:[0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9
*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Computed a valid PMKID from MSCB PMK cache for
***The new PMKID is computed and validated to match the one provided by the client, which is also compu

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Setting active key cache index 0 ---> 0

*apfMsConnTask_2: Jun 21 21:48:50.564: 00:40:96:b7:ab:5c Sending Assoc Response to station on BSSID 84:
***The Reassociation response is sent to the client, which validates the fast-roam with PKC/OKC.

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c Initiating RSN with existing PMK to mobile 00:40:
***WLC initiates a Robust Secure Network association with this client-and AP pair with the cached PMK f

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c Skipping EAP-Success to mobile 00:40:96:b7:ab:5c

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c Found an cache entry for BSSID 84:78:ac:f0:2a:92 

*dot1xMsgTask: Jun 21 21:48:50.570: Including PMKID in M1  (16)
***The hashed PMKID is included on the Message-1 of the WPA/WPA2 4-Way handshake.

*dot1xMsgTask: Jun 21 21:48:50.570: [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9
***The PMKID is hashed. The next messages are the same WPA/WPA2 4-Way handshake messages described thus

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c Sending EAPOL-Key Message to mobile 00:40:96:b7:a

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5 Received EAPOL-Key from mobile 00:40:96:b7:a

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5c Received EAPOL-key in PTK_START state (mess

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5cPMK: Sending cache add

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.590: 00:40:96:b7:ab:5c Sending EAPOL-Key Message to mobile 00:40:9

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.610: 00:40:96:b7:ab:5c Received EAPOL-Key from mobile 00:40:96:b7:
```

```
*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.610: 00:40:96:b7:ab:5c Received EAPOL-key in PTKINITNEGOTIATING st
```

As shown at the start of the debugs, the PMKID must be computed after the Reassociation Request from the client is received. This is needed in order to validate the PMKID and confirm that the cached PMK is used with the WPA2 4-Way handshake to derive the encryption keys and finish the fast-secure roaming. Do not confuse the CCKM entries on the debugs; this is not used in order to perform CCKM, but PKC/OKC, as previously explained. Here CCKM is simply a name used by the WLC for those outputs, such as the name of a function that handles the values in order to compute the PMKID.

Scenario 23: Verify Fast-Secure-Roaming (FSR) with 802.11r

Debug used:

debug client <mac addr>

```
*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32 Doing preauth for this client over the Air
***WLC begins FT fast-secure roaming over-the-Air with this client and performs a type of preauthentica
because the client asks for this with FT on the Authentication frame that is sent to the new AP over-th

*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32 Doing local roaming for destination address 84
***WLC performs the local roaming event with the new AP to      which the client roams.

*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32 Got 1 AKMs in RSNIE
*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32 RSNIE AKM matches with PMK cache entry :0x3
***WLC receives one PMK from this client (known as AKM here), which matches the PMK cache entry hold fo

*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32 Created a new preauth entry for AP:84:78:ac:f0
*apfMsConnTask_2: Jun 27 19:25:48.751: Adding MDIE,   ID is:0xaaf0
***WLC creates a new preauth entry for this AP-and-Client pair, and adds the MDIE information.

*apfMsConnTask_2: Jun 27 19:25:48.763: Processing assoc-req station:ec:85:2f:15:39:32 AP:84:78:ac:f0:2a
*apfMsConnTask_2: Jun 27 19:25:48.763: ec:85:2f:15:39:32 Reassociation received from mobile on BSSID 84
***Once the client receives the Authentication frame reply from the WLC/AP, the Reassociation request i

*apfMsConnTask_2: Jun 27 19:25:48.764: ec:85:2f:15:39:32 Marking this mobile as TGr capable.

*apfMsConnTask_2: Jun 27 19:25:48.764: ec:85:2f:15:39:32 Processing RSN IE type 48, length 38 for mobil

*apfMsConnTask_2: Jun 27 19:25:48.765: ec:85:2f:15:39:32 Roaming succeed for this client.
***WLC confirms that the FT fast-secure roaming is successful for this client.

*apfMsConnTask_2: Jun 27 19:25:48.765: Sending assoc-resp station:ec:85:2f:15:39:32 AP:84:78:ac:f0:2a:9
*apfMsConnTask_2: Jun 27 19:25:48.766: Adding MDIE, ID is:0xaaf0
*apfMsConnTask_2: Jun 27 19:25:48.766: ec:85:2f:15:39:32 Including FT Mobility Domain IE (length 5) in
*apfMsConnTask_2: Jun 27 19:25:48.766: ec:85:2f:15:39:32 Sending Assoc Response to station on BSSID 84:
***The Reassociation response is sent to the client, which includes the FT Mobility Domain IE.

*dot1xMsgTask: Jun 27 19:25:48.769: ec:85:2f:15:39:32 Finishing FT roaming for mobile ec:85:2f:15:39:32
***FT roaming finishes and EAP is skipped (as well as any other key management handshake), so the clien

*dot1xMsgTask: Jun 27 19:25:48.769: ec:85:2f:15:39:32 Skipping EAP-Success to mobile ec:85:2f:15:39:32
```

.